Solution Integration Guide for Communication Server 1000/ Business Communications Manager

CS 1000/BCM

Document Number: **NN43001-326**

Document Status: **Standard**

Document Version: **01.02**

Date: **25 October 2006**

NORTEL

Copyright © 2006 Nortel Networks. All Rights Reserved.

Sourced in Canada.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, Nortel (Logo), the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Contents

Contents 3

How to get help 5
- Finding the latest updates on the Nortel Web site 5
- Getting help from the Nortel Web site 6
- Getting help over the phone from a Nortel Solutions Center 6
- Getting help from a specialist by using an Express Routing Code 7
- Getting help through a Nortel distributor or reseller 7

About this document 9
- Audience 9
- Symbols and conventions 9
- Related information 9

Overview 11

Prerequisites 15
- Knowledge requirements 15
  - Training 15
- Capturing integration parameters 15
- Establishing the system baseline 17

CS 1000 setup and IP Peer Networking configuration 23
- CS 1000/IP Peer Networking configuration procedures 23
- H.323 Call Server configuration 24
  - Defining the customer to support ISDN 24
  - Creating the virtual D-channel 27
  - Configuring the zones in LD 117 29
  - Creating the virtual route (LD 16) 30
  - Creating the virtual trunks (LD 14) 32
  - Creating the ESN data block for CDP 34
  - Creating the Network Control Block (NCTL) for network access (LD 87) 36
  - Creating the RLB for the virtual trunk route (LD 86) 37
  - Creating the CDP steering codes (LD 87) 38
  - Checking CODEC and QoS settings 39
- H.323 Gatekeeper Configuration 41
  - Configuring Element Manager 41
- SIP protocol configuration 43
  - SIP addressing and Universal Resource Identifier 43
    - SIP Gateway URI mapping and addressing 43
  - Configuration for the SIP protocol 44
  - Enabling the SIP Virtual Trunk application 45

Configuring the SIP Gateway 45
Configuring the SIP Redirect Server and URI map 47
Configuring IP networking for SIP 48
Defining the customer to support ISDN 48
Creating the virtual D-channel 48
Configuring the zones in LD 117 49
Creating the virtual route (LD 16) 50
Creating the virtual trunks (LD 14) 52
Creating the ESN data block for CDP 54
Creating the Network Control Block (NCTL) for network access (LD 87) 55
Creating the RLB for the virtual trunk route (LD 86) 55
Creating the CDP steering codes (LD 87) 56
Checking CODEC and QoS settings 57

NRS configuration 59
NRS configuration procedures 59
Enabling NRS 59
Launching NRS Manager 61
Verifying and adjusting system-wide settings 62
Configuring the NRS server settings (H.323 Gatekeeper or SIP) 64
Configuring the service domain 66
Configuring the L1 domain (UDP) 67
Configuring the L0 domain (CDP) 70
Configuring Gateway endpoints 74
Configuring routing entries 78
Configuring collaborative servers 80
Updating the database 81
Checking the status of registered endpoints 82
Performing an H.323 routing test 83
Checking the status of virtual D-channels 84
Checking the status of virtual trunks 85
Committing Gatekeeper configuration changes 86

BCM 200/400 configuration 89
BCM 200/400 configuration procedures 89
Configuring incoming VoIP trunks 89
Verifying system license and keycodes 90
Configuring VoIP trunk media parameters 90
Configuring local Gateway parameters 94
Configuring VoIP lines 99
Configuring target lines 103

Testing and troubleshooting 107
Testing 107
Testing the integration from the BCM system 107
Testing the integration from the CS 1000 system 108
Troubleshooting 108
BCM is unable to contact the gatekeeper at <IP address> 108
Unable to complete any calls 109
Cannot make calls between the CS 1000 and BCM 109
BCM fails to register to NRS 109
H.323 Gateway service is down 110

How to get help

This chapter explains how to get help for Nortel products and services.

Finding the latest updates on the Nortel Web site

The content of this documentation is current at the time of product release. To check for updates to the latest documentation and software for Communication Server 1000 and Business Communications Manager (BCM), click one of the following links:

Link	Takes you directly to the
Latest CS 1000E software	Nortel page for CS 1000E software located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=14261
Latest CS 1000M Cabinet/Chassis software	Nortel page for CS 1000M Cabinet/Chassis software located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=12515
Latest CS 1000M Half Group/Single Group/ Multi-Group software	Nortel page for CS 1000M Half Group/Single Group/ Multi-Group software located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=12516
Latest CS 1000S software	Nortel page for CS 1000S software located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=12514
Latest BCM 200 software	Nortel page for BCM 200 software located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=8236
Latest BCM 400 software	Nortel page for BCM 400 software located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=17141

Link	Takes you directly to the
Latest CS 1000E documentation	Nortel page for CS 1000E documentation located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=DOCUMENTATION&resetFilter=1&poid=14261
Latest CS 1000M Cabinet/Chassis documentation	Nortel page for CS 1000M Cabinet/Chassis documentation located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=DOCUMENTATION&resetFilter=1&poid=12515
Latest CS 1000M Half Group/Single Group/ Multi-Group documentation	Nortel page for CS 1000M Half Group/Single Group/ Multi-Group documentation located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=DOCUMENTATION&resetFilter=1&poid=12516
Latest CS 1000S documentation	Nortel page for CS 1000S documentation located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=DOCUMENTATION&resetFilter=1&poid=12514
Latest BCM 200 documentation	Nortel page for BCM 200 documentation located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=DOCUMENTATION&resetFilter=1&poid=8236
Latest BCM 400 documentation	Nortel page for BCM 400 documentation located at: http://www130.nortelnetworks.com/go/main.jsp?cscat=DOCUMENTATION&resetFilter=1&poid=17141

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchase a service contract for your Nortel product from a distributor or authorized reseller, you can contact the technical support staff for that distributor or reseller.

About this document

This document describes the planning, configuration, and troubleshooting of the integration of the Business Communications Manager (BCM) with a Communication Server 1000 system. Integrate the CS 1000 and BCM systems when both systems have been installed and a baseline of operation has been achieved and tested.

The following systems and software releases are covered in this guide:

- Communication Server 1000 Release 4.5
- Business Communications Manager 200 Release 4.0
- Business Communications Manager 400 Release 4.0

This document is intended to be a stand-alone guide, covering the prerequisites to and implementation of a successful CS 1000/BCM integration. A minimum skill set and level of understanding is assumed. References to other NTPs, engineering guides, or troubleshooting guides are made for informational purposes.

Audience

The intended audience for this document includes installation, planning, and maintenance personnel.

Symbols and conventions

The following symbols are used in this document.

Note: A note alerts you to important or related information.

Tip: Tips or suggestions on additional sources of information or shortcuts are provided. Any potential problems that may arise are also identified.

Related information

The following NTPs are referenced in this guide:

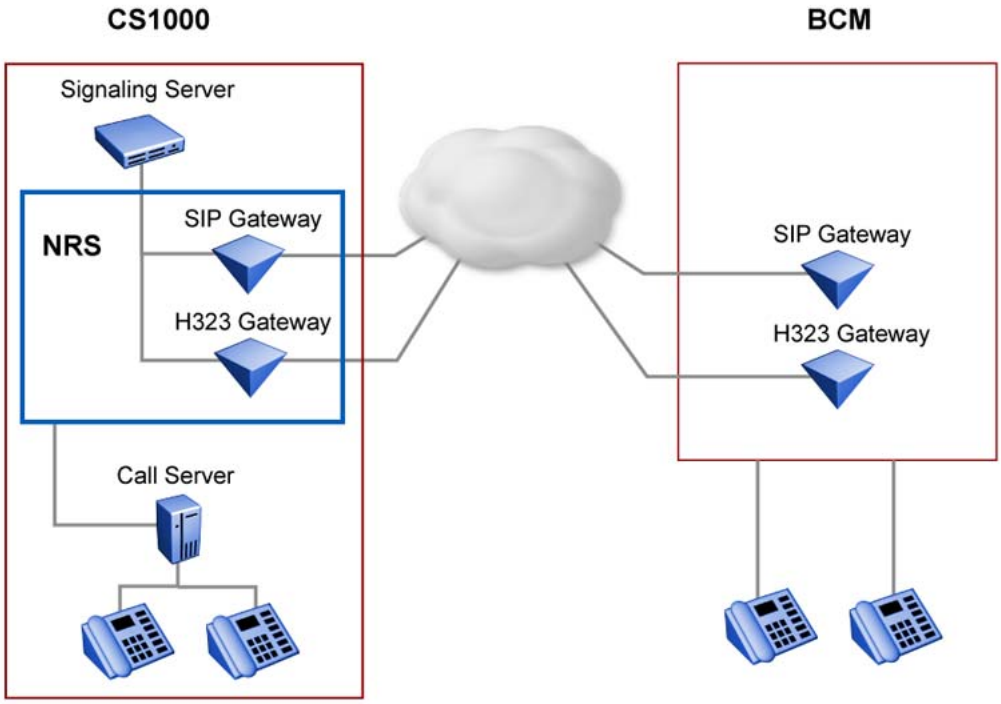
- *BCM 4.0 Device Configuration Guide* (N0060600)
- *BCM 4.0 Telephony Device Installation Guide* (N0060609)
- *Communication Server 1000E: Installation and Configuration* (553-3041-210)

- *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)
- *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210)
- *Communication Server 1000S: Installation and Configuration* (553-3031-210)
- *Dialing Plans: Description* (553-3001-183)
- *IP Line Description, Installation, and Maintenance* (553-3001-365)
- *IP Peer Networking Installation and Configuration Guide* (553-3001-213)
- *Keycode Installation Guide* (NN40010-301)
- *Signaling Server: Installation and Configuration* (553-3001-212)

Overview

An example of a Communication Server 1000/Business Communications Manager (BCM) systems integration is shown in Figure 1 "Architecture".

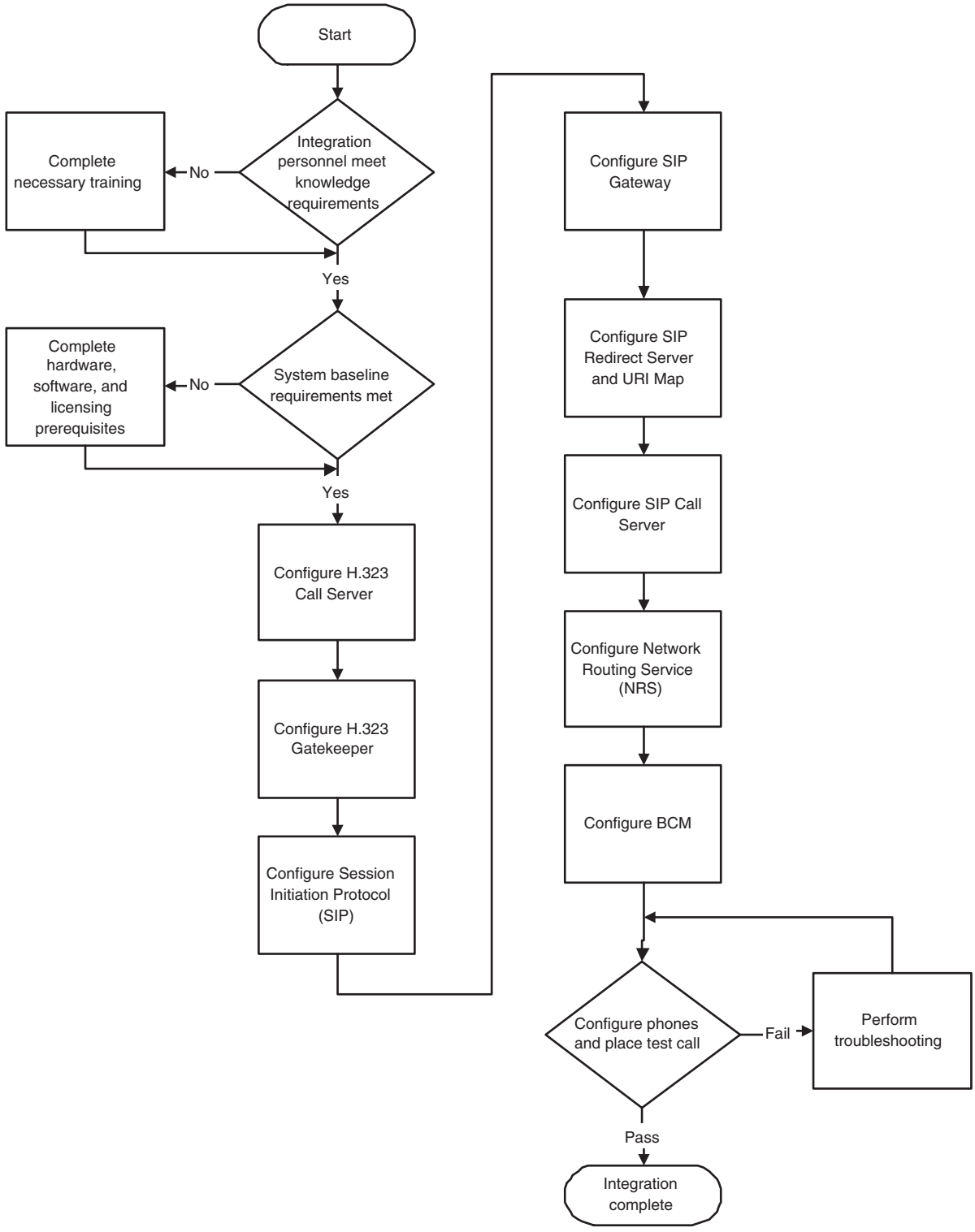
Figure 1 Architecture



CS 1000 Gateway IP address	192.167.102.1	
CS 1000 Endpoint IP address	192.167.103.2	
BCM 400 Endpoint IP address	192.168.249.27	BCM Gateway Alias name BCM40
Signaling Server T-LAN IP Address	192.167.103.3	
Signaling Server E-LAN IP address	192.167.102.4	
Call Server E-LAN IP Address	192.167.102.3	
NRS IP Address	192.167.103.2	NRS Host name CS1000E_PIV
NCS IP Address	192.167.103.3	
BCM IP Address	192.168.249.27	

Figure 2 "CS 1000/BCM integration process" (page 12) shows the sequence of procedures you perform to integrate the CS 1000 and BCM systems.

Figure 2 CS 1000/BCM integration process



The tasks in the CS 1000/BCM systems integration process are listed in Table 1 "Task Completion Checklist" . Use this checklist to implement the integration.

Table 1 Task Completion Checklist (Sheet 1 of 2)

☑	Task	Reference
	Configure the H.323 Call Server	**1** "Defining the customer to support ISDN " (page 24) **2** "Creating the virtual D-channel" (page 27) **3** "Configuring the zones in LD 117" (page 29) **4** "Creating the virtual route (LD 16)" (page 30) **5** "Creating the virtual trunks (LD 14)" (page 32) **6** "Creating the ESN data block for CDP" (page 34) **7** "Creating the Network Control Block (NCTL) for network access (LD 87)" (page 36) **8** "Creating the RLB for the virtual trunk route (LD 86)" (page 37) **9** "Creating the CDP steering codes (LD 87)" (page 38) **10** "Checking CODEC and QoS settings" (page 39)
	Configure the H.323 Gatekeeper	"Configuring Element Manager" (page 41)
	Configure SIP Protocol	"Enabling the SIP Virtual Trunk application" (page 45)
	Configure the SIP Gateway	"Configuring the SIP Gateway" (page 45)
	Configure the SIP Redirect Server and URI Map	"Configuring the SIP Redirect Server and URI map" (page 47)
	Configure the SIP Call Server	**1** "Defining the customer to support ISDN " (page 48) **2** "Creating the virtual D-channel" (page 48) **3** "Configuring the zones in LD 117" (page 49) **4** "Creating the virtual route (LD 16)" (page 30) **5** "Creating the virtual trunks (LD 14)" (page 52) **6** "Creating the Network Control Block (NCTL) for network access (LD 87)" (page 55) **7** "Creating the RLB for the virtual trunk route (LD 86)" (page 55) **8** "Creating the CDP steering codes (LD 87)" (page 56) **9** "Checking CODEC and QoS settings" (page 57)

Table 1 Task Completion Checklist (Sheet 2 of 2)

☑	Task	Reference
	Configure NRS	**1** "Enabling NRS" (page 59) **2** "Launching NRS Manager" (page 61) **3** "Verifying and adjusting system-wide settings" (page 62) **4** "Configuring the NRS server settings (H.323 Gatekeeper or SIP)" (page 64) **5** "Configuring the service domain" (page 66) **6** "Configuring the L1 domain (UDP)" (page 67) **7** "Configuring the L0 domain (CDP)" (page 70) **8** "Configuring Gateway endpoints" (page 74) **9** "Configuring routing entries" (page 78) **10** "Configuring collaborative servers" (page 80) **11** "Updating the database" (page 81) **12** "Checking the status of registered endpoints" (page 82) **13** "Performing an H.323 routing test" (page 83) **14** "Checking the status of virtual D-channels" (page 84) **15** "Checking the status of virtual trunks" (page 85) **16** "Committing Gatekeeper configuration changes" (page 86)
	Configure BCM	**1** "Configuring incoming VoIP trunks" (page 89) **2** "Verifying system license and keycodes" (page 90) **3** "Configuring VoIP trunk media parameters" (page 90) **4** "Configuring local Gateway parameters" (page 94) **5** "Configuring VoIP lines" (page 99) **6** "Configuring target lines" (page 103)
	Test and troubleshoot integration	"Testing and troubleshooting" (page 107)

Prerequisites

Before you begin to integrate the Business Communications Manager (BCM) and Communication Server 1000 systems, ensure that you complete the following prerequisites:

- "Knowledge requirements" (page 15)
- "Capturing integration parameters" (page 15)
- "Establishing the system baseline" (page 17)

Knowledge requirements

The following knowledge and skills are required to implement a CS 1000/BCM systems integration:

- basic programming and provisioning skills for the CS 1000 system
- basic programming and provisioning skills for Network Routing Service (NRS)
- working knowledge of establishing dialing plans
- basic programming and provisioning skills for BCM systems
- working knowledge of various operating systems, including VxWorks, Unix, Linux, and Windows
- principles of Voice over IP (VoIP) protocols
- networking principles
- knowledge of core data components

Training

Nortel recommends that you complete product-specific training before you begin integrating the CS 1000 and BCM systems. Training includes Course 6034C, “CS 1000 BCM Multi-site Integration”, which deals specifically with the CS 1000/ BCM integration and multi-site BCM integration processes. A complete list of courses is available at www.nortel.com.

Capturing integration parameters

Table 2 "Integration Parameters" (page 16) provides a list of parameters required to successfully complete the integration. Record these parameters during the initial planning phase of the integration.

Table 2 Integration Parameters

Parameter	Value
Service domain name in NRS	
Coordinated Dialing Plan steering codes	
Gatekeeper IP address	
Alternate Gatekeeper IP address (optional)	
T-LAN IP address of Signaling Server	
T-LAN IP address of alternate Signaling Server	
H.323 ID (preferable if it is the same as the one in the Primary Signaling Server)	
SIP access port to use (port 5060 is recommended)	
SIP domain name (must be the same as the service domain name)	
SIP Gateway endpoint name (must match the NRS user ID)	
SIP Gateway endpoint authentication password (must match the NRS password)	
L1 domain name	
L0 domain name	
H.323 Gatekeeper alias name (default is the H.323 ID)	
Primary SIP proxy address	
Alternate SIP proxy address	
Primary NCS IP address	
Alternate NCS IP address	
Read and write community names	
Static endpoint IP address (same as the Node IP address)	
Collaborative server IP address	
End Point alias for BCM	

Establishing the system baseline

To successfully integrate voice services, you must first establish the system baseline for the Call Server, Signaling Server, and Business Communications Manager (BCM) so that the systems are configured and working in a stand-alone environment.

Use Table 3 "Pre-integration checklist" to complete system baselines prior to integration.

Table 3 Pre-integration checklist (Sheet 1 of 6)

☑	Task	Reference	Comments
	The Enterprise software package is purchased and installed, with appropriate licenses for virtual trunks, lines, and IP Phones as required.		
	The Network Numbering Plan is implemented.	*Dialing Plans: Description* (553-3001-183)	Are you using a Uniform Dialing Plan (UDP) or a Coordinated Dialing Plan (CDP), or both? Are you also using a Group Dialing Plan (GDP), a North American Numbering Plan (NANP), or a Flexible Numbering Plan (FNP)?
	CS 1000 software is Release 4.5 or later.		To check the CS 1000 software release: Log on, enter LD 22, and type PRT ISS OR **1** Log on to Element Manager. **2** On the left navigation pane, select **Home**. The Home System View page appears. **3** In the Call Server section, the software release is referred to as Release.

Table 3 Pre-integration checklist (Sheet 2 of 6)

☑	Task	Reference	Comments
	Signaling Server software is Release 4.5 or later.		The Signaling Server software should be the most recent GA release compatible with your Call Server software version. To check the software release of the Signaling Server: **1** Log on to Element Manager. **2** On the left navigation pane, select **Home**. The Home System view page appears. **3** Refer to the Signaling Server section for the Software Version.
	Basic installation, setup, and configuration of the Call Server components and the Signaling Server are complete.	*Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210) *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)— *Communication Server 1000S: Installation and Configuration* (553-3031-210) *Communication Server 1000E: Installation and Configuration* (553-3041-210) *Signaling Server: Installation and Configuration* (553-3001-212)	
	Primary, alternate, and fail-safe Network Routing Service (NRS) are configured at installation and initial setup of the Signaling Server.	*Signaling Server: Installation and Configuration* (553-3001-212)	The NRS requires IP telephony node configuration files. These files are installed and configured during the Signaling Server software installation as a basic configuration step.

Table 3 Pre-integration checklist (Sheet 3 of 6)

☑	Task	Reference	Comments
	Digital Data Block configuration is complete in LD 73.	*IP Peer Networking Installation and Configuration Guide* (553-3001-213)	To configure a Digital Data Block: **1** Log on to the Call Server and enter LD 73. **2** Enter **New**. **3** Enter **DDB**. **4** Press Enter to accept all defaults. **5** Perform a data dump
	PTI or DTI trunks (DLOP) configuration is complete in LD 17.	*IP Peer Networking Installation and Configuration Guide* (553-3001-213)	To check PTI or DTI trunks: **1** Log on to Element Manager. **2** Select **Routes and Trunks > Digital Trunk Interface**. **3** Select **Digital Trunk Interface Data Block**. **4** Check that the configuration is complete.
	A basic node is configured in Element Manager.	*IP Line Description, Installation, and Maintenance* (553-3001-365)	This node information is updated through the integration process.
	Voice Gateway Media Card configuration is complete if IP to PSTN translation is required.		To check that Media Gateway Cards are installed: **1** Log on to Element Manager. **2** On the left side navigation pane, expand the **IP Telephony** tab. **3** Expand the **Software** tab. **4** Select **Servers and Media Cards**. The Servers and Media View page appears. **5** Select **Open all Nodes**. **Attention:** The servers and Media Cards installed and configured are listed under each node. Any installed Voice Gateway Media Card is listed under Type.

Table 3 Pre-integration checklist (Sheet 4 of 6)

☑	Task	Reference	Comments
	H.323 Virtual Trunk package 399 is installed.		To check that the package is loaded: **1** Open a telnet session to the Call Server. **2** Log on to the Signaling Server. **3** Enter **LD 22**. **4** Enter **PRT**. **5** Enter **PKG 399**. **6** The package is loaded if you do not receive a “package is restricted” message.
	IPT is Release 3.0 or newer if you are using IP Trunk cards.		To check that IPT Trunk cards are installed: **1** Log on to Element Manager. **2** On the left navigation pane, expand the **IP Telephony** tab. **3** Expand the **Software** tab. **4** Select **Servers and Media Cards**. The Servers and Media View page appears. **5** Select **Open all Nodes**. **Attention:** The servers and Media Cards installed and configured are listed under each node. Any installed IPT Trunk cards are listed under Type.
	BCM configuration is complete and passing data traffic.		
	BCM networking hardware is installed for integration.		To check the installed hardware: **1** Log on to Element Manager. **2** Select the **Administration** tab. **3** Expand the **General** folder. **4** Select **Hardware Inventory**. **5** Select the **PCI Cards** tab. The cards installed in BCM are listed.

Table 3 Pre-integration checklist (Sheet 5 of 6)

☑	Task	Reference	Comments
	PEC III Media Service Cards (MSC) are later.		PECIII MSCs are required for T.38 Fax and IP telephony. To check the PEC hardware: **1** Log on to Element Manager. **2** Select the **Administration** tab. **3** Expand the **General** folder. **4** Select **Hardware Inventory**. **5** Select the **PCI Cards** tab. **6** Select the **MSC PCI card** and scroll down to the **Details for Card** section.
	BCM 200/400 is Release 4.0 or later.		To check the software version: **1** Log on to Element Manager. **2** Select the **Configuration** tab. **3** Expand the **System** folder. **4** Select **Identification**.
	BCM 50 is version 2.0 or later.		To check the software version: **1** Log on to Element Manager. **2** Select the **Configuration** tab. **3** Expand the **System** folder. **4** Select **Identification**.
	BCM on the same network as the systems being integrated are release 3.5 or later		To check the software version: **1** Log on to Element Manager. **2** Select the **Configuration** tab. **3** Expand the **System** folder. **4** Select **Identification**.
	VoIP Gateway Trunk licensing is purchased and loaded on BCM.	*Keycode Installation Guide* (NN40010-301)	To check Feature Licenses: **1** Log on to Element Manager. **2** Select the **Configuration** tab. **3** Expand the **System** folder. **4** Select **Keycode**.

Table 3 Pre-integration checklist (Sheet 6 of 6)

☑	Task	Reference	Comments
	IP Client licensing is purchased and loaded on BCM.	*Keycode Installation Guide* (NN40010-301)	To check Feature Licenses: **1** Log on to Element Manager. **2** Select the **Configuration** tab. **3** Expand the **System** folder. **4** Select **Keycode**.
	MCDN feature licensing is purchased and loaded on BCM.	*Keycode Installation Guide* (NN40010-301)	To check Feature Licenses: **1** Log on to Element Manager. **2** Select the **Configuration** tab. **3** Expand the **System** folder. **4** Select **Keycode**.

CS 1000 setup and IP Peer Networking configuration

Although you can configure the Communication Server 1000 and IP Peer Networking through overlays, the use of Element Manager and Network Routing Services (NRS) Manager are recommended. The Element Manager Web server resides on the Signaling Server and you can access it directly through a Web browser or by using Optivity Telephony Manager (OTM). You must configure NRS through Network Routing Service Manager (NRS Manager), which you can access only through the Element Manager.

Configure the Call Server through Element Manager in the following order:

- H.323 Call Server
- H.323 Gate Keeper
- SIP
  - SIP Protocol
  - SIP Gateway
  - SIP Redirect Server and URI Map
  - SIP Call Server
  - Network Routing Service in the NRS Manager
  - SIP addressing
  - SIP Virtual Trunking

CS 1000/IP Peer Networking configuration procedures

The sequence of CS 1000/IP Peer Networking configuration procedures is as follows:

- "H.323 Call Server configuration" (page 24)
  - "Defining the customer to support ISDN " (page 24)
  - "Creating the virtual D-channel" (page 27)
  - "Configuring the zones in LD 117" (page 29)
  - "Creating the virtual route (LD 16)" (page 30)
  - "Creating the virtual trunks (LD 14)" (page 32)
  - "Creating the ESN data block for CDP" (page 34)
  - "Creating the Network Control Block (NCTL) for network access (LD 87)" (page 36)
  - "Creating the RLB for the virtual trunk route (LD 86)" (page 37)

  - "Creating the CDP steering codes (LD 87)" (page 38)
  - "Checking CODEC and QoS settings" (page 39)
- "H.323 Gatekeeper Configuration" (page 41)
  - "Configuring Element Manager" (page 41)
- "SIP protocol configuration" (page 43)
  - "Enabling the SIP Virtual Trunk application" (page 45)
  - "Configuring the SIP Gateway" (page 45)
  - "Configuring the SIP Redirect Server and URI map" (page 47)
  - "Configuring IP networking for SIP" (page 48)
  - "Defining the customer to support ISDN " (page 48)
  - "Creating the virtual D-channel" (page 48)
  - "Configuring the zones in LD 117" (page 49)
  - "Creating the virtual route (LD 16)" (page 30)
  - "Creating the virtual trunks (LD 14)" (page 52)
  - "Creating the ESN data block for CDP" (page 54)
  - "Creating the Network Control Block (NCTL) for network access (LD 87)" (page 55)
  - "Creating the RLB for the virtual trunk route (LD 86)" (page 55)
  - "Creating the CDP steering codes (LD 87)" (page 56)
  - "Checking CODEC and QoS settings" (page 57)

H.323 Call Server configuration

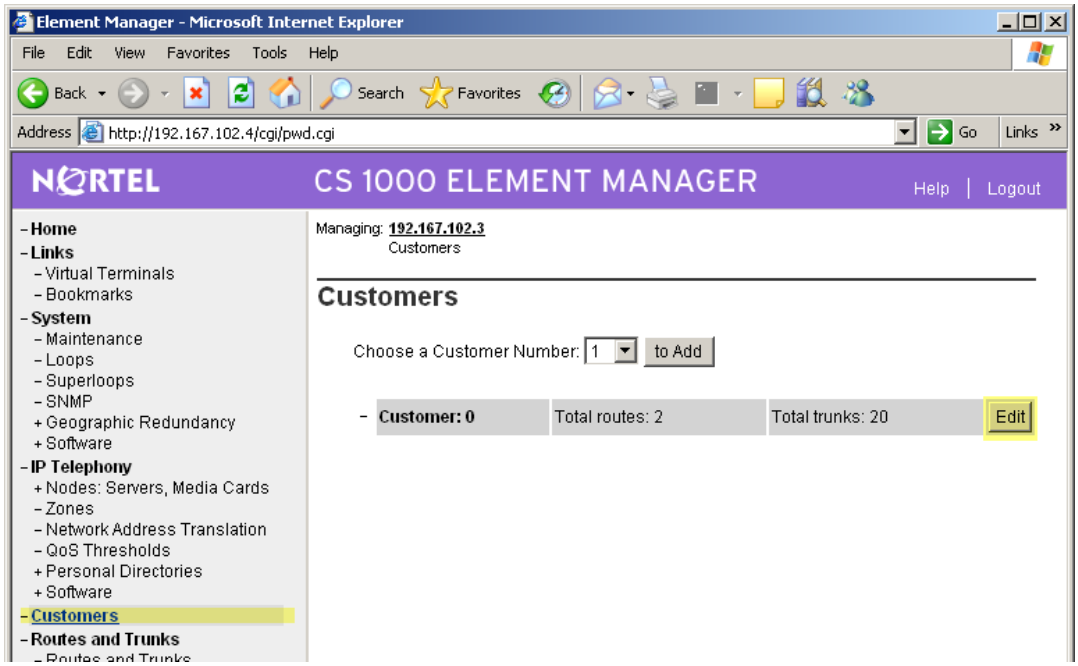
Complete the following steps for each Call Server in your IP Peer Network:

- "Defining the customer to support ISDN " (page 24)
- "Creating the virtual D-channel" (page 27)
- "Configuring the zones in LD 117" (page 29)
- "Creating the virtual route (LD 16)" (page 30)
- "Creating the virtual trunks (LD 14)" (page 32)
- "Creating the ESN data block for CDP" (page 34)
- "Creating the Network Control Block (NCTL) for network access (LD 87)" (page 36)
- "Creating the RLB for the virtual trunk route (LD 86)" (page 37)
- "Creating the CDP steering codes (LD 87)" (page 38)
- "Checking CODEC and QoS settings" (page 39)

Defining the customer to support ISDN

Step	Action
1	Log on to Element Manager.
2	In the left navigation pane, select **Customers**. See Figure 3 "Customers" (page 25).

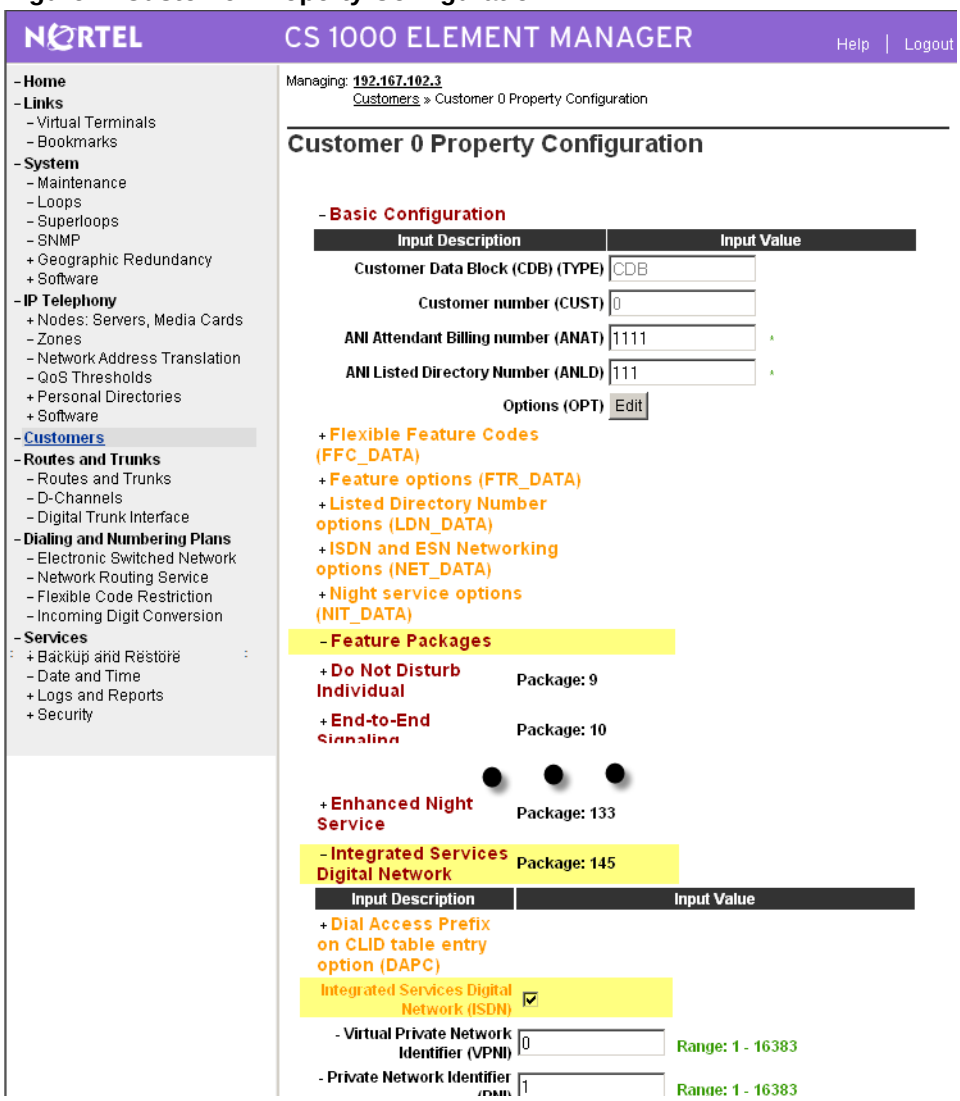
Figure 3 Customers



3 Click the **Edit** button.

The Customer Property Configuration page appears. See Figure 4 "Customer Property Configuration" (page 26).

Figure 4 Customer Property Configuration



4 Expand the **Feature Packages** heading.

5 Expand the **Integrated Services Digital Network Package 145** heading.

The ISDN parameters are displayed.

6 Select the **Integrated Services Digital Network (ISDN)** check box.

7 At the bottom of the page, click **Submit**.

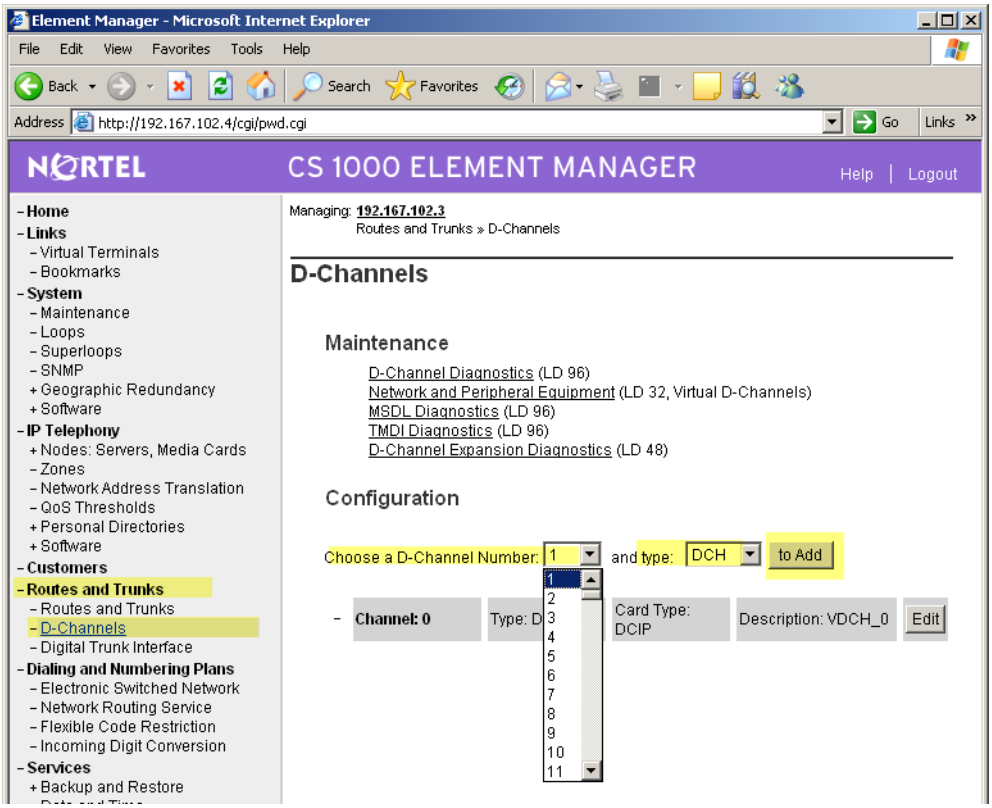
End

Creating the virtual D-channel

Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > D-Channels**. The D-Channels page appears. See Figure 5 "D-Channels".

Note: If a D-Channel is not configured, the following message appears: Do not have any D-Channel configured in the system! To add a new D-Channel, click on [OK]. [H0046]

Figure 5 D-Channels



3 From the **Choose a D-Channel Number** menu, select the D-Channel number.

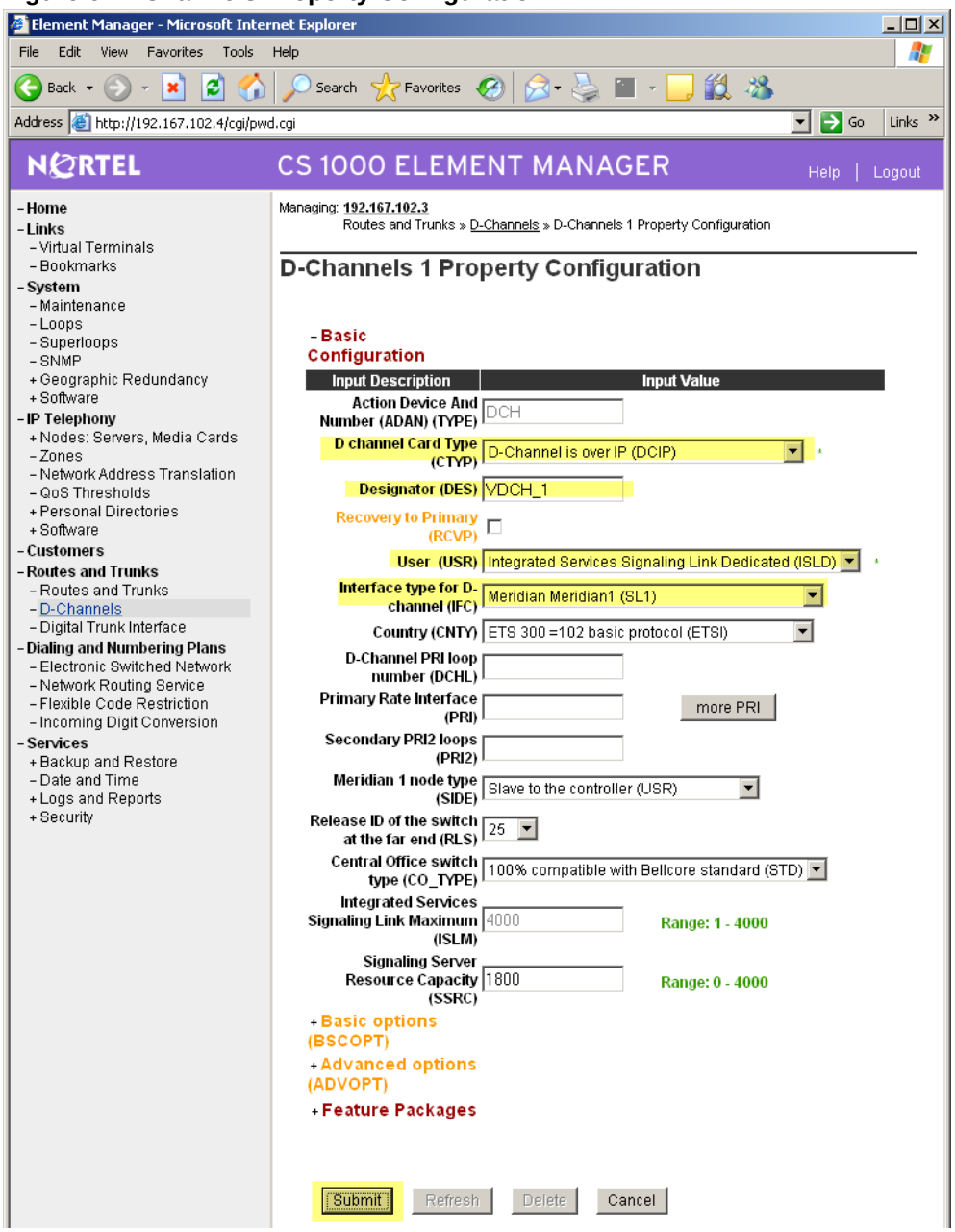
D-channels 0,1, and 2 are usually used or shared with other applications. It is recommended that you begin configuring virtual D-channels on channel 3.

4 From the **Type** menu, select the D-Channel type.

5 Click **to Add**.

The D-Channels Property Configuration page appears. See Figure 6 "D-Channels Property Configuration" (page 28).

Figure 6 D-Channels Property Configuration



6 For the **D Channel Card Type (CTYP)**, select **D-channel is over IP (DCIP)**.

7 For the **Designator (DES)**, type a meaningful name. The Designator must not contain spaces; use underscores instead.

Make a note of the Designator in your records for future reference.

8 For **User (USR)**, select **Integrated Services Signaling Link Dedicated (ISLD)**.

9 For **Interface type for D-channel (IFC)**, select **Meridian Meridian1 (SL1)**.

10 Leave all other parameters as is and click **Submit**.

The new channel appears.

End

Configuring the zones in LD 117

Before you can configure the virtual routes and trunks, the following zones must be configured, in any order:

- Zone 1 = IP Phones zone (ZBRN = MO)
- Zone 2 = Voice Gateway Channels zone, which should be different from the IP Phones zone (ZBRN = VTRK)

Ensure that enough bandwidth is allocated for the zones with the heaviest traffic.

Never use or configure zone 0.

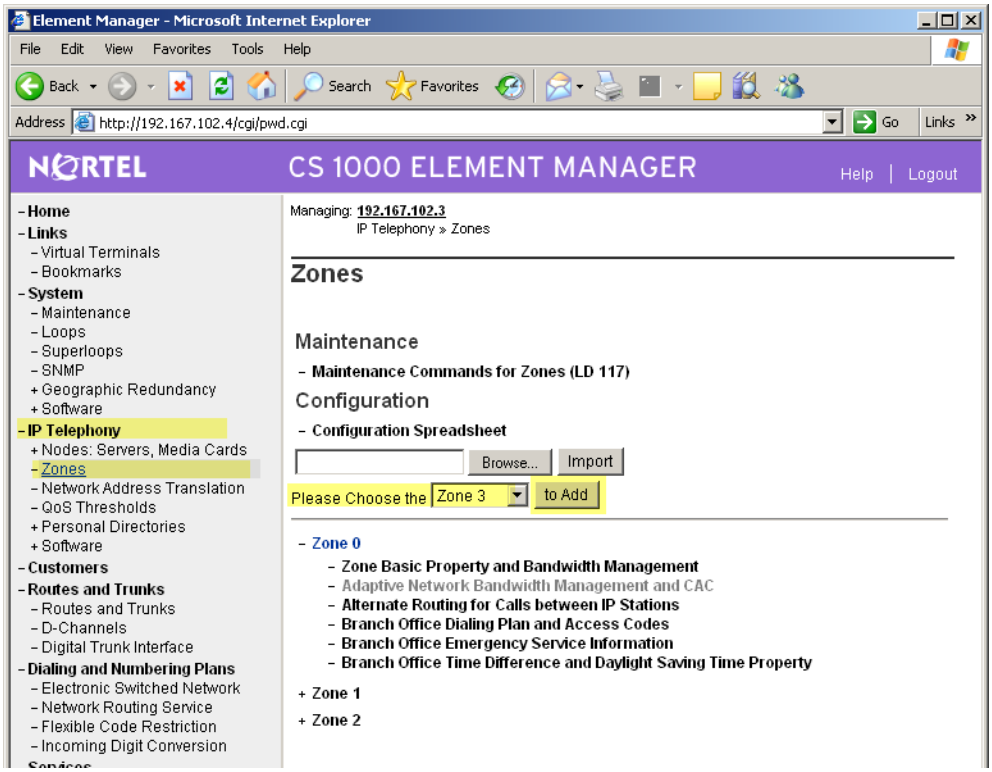
Step	Action

1 Log on to Element Manager.

2 Select **IP Telephony > Zones**.

See Figure 7 "Zones".

Figure 7 Zones



3 Select **Zone 1**.

Note: If Zone 1 is configured, it appears in the list of configured zones at the bottom of the page.

4 Click **to Add**.

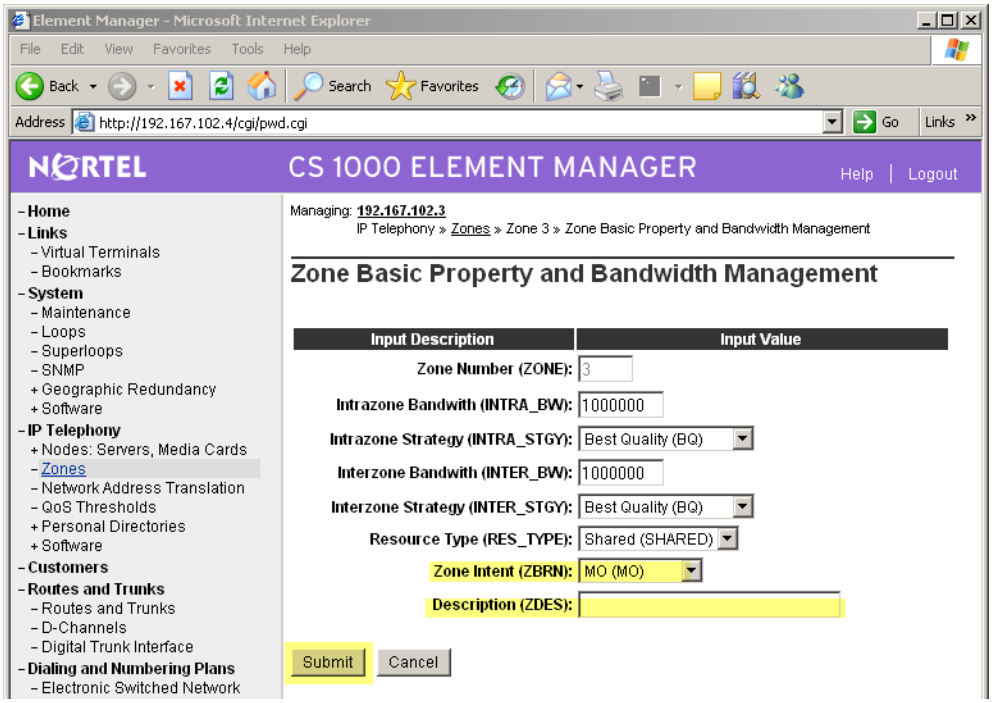
The Zone Basic Property and Bandwidth Management page appears. See Figure 8 "Zone Basic Property and Bandwidth Management".

Note: The following message may appear after you click **to Add**:

To maintain consistent zone properties within the network, it is recommended to use the “Zone Basic Property and Bandwidth Management Spreadsheet”. Do you wish to proceed?

Click the **OK** button.

Figure 8 Zone Basic Property and Bandwidth Management



5 Leave the default values for bandwidth and resource type as is.

6 Set the **Zone Intent (ZBRN)** as follows:

- Zone 1 is for the IP Phones at the Main Office. Set Zone Intent (ZBRN) for Zone 1 to **MO**.
- Zone 2 is for the Voice Gateway Channels. Set Zone Intent (ZBRN) for Zone 2 to **VTRK**.

7 For **Description (ZDES)**, type a meaningful description.

8 Click **Submit**.

9 Repeat for Zones 2 and 3.

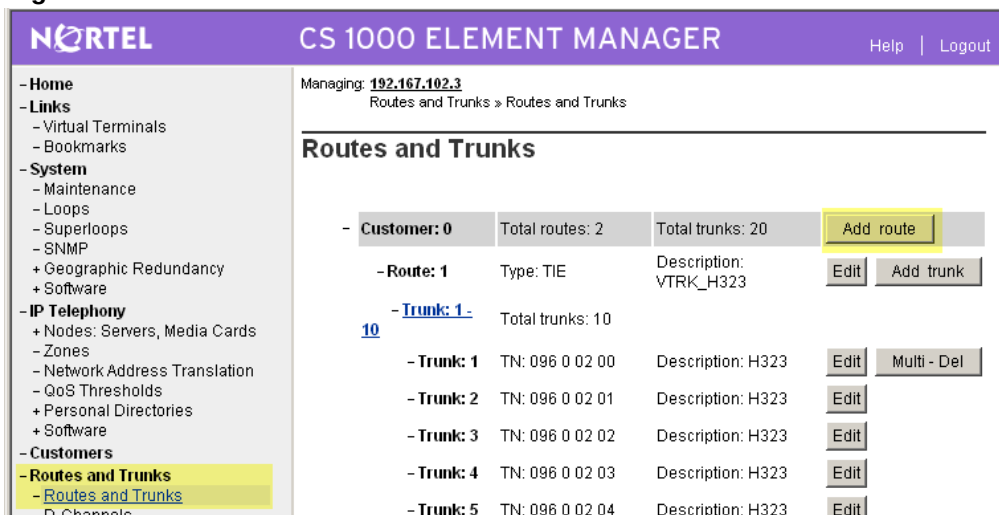
End

Creating the virtual route (LD 16)

Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > Routes and Trunks**.

See Figure 9 "Routes and Trunks".

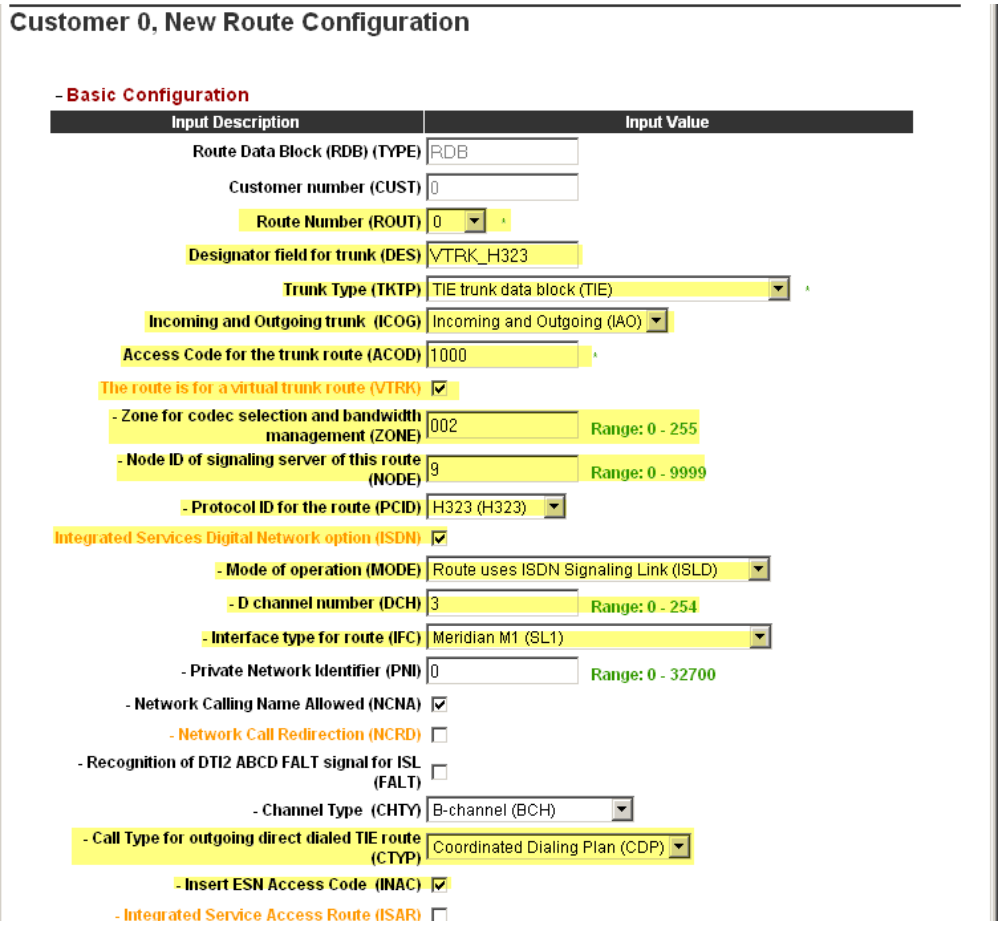
Figure 9 Routes and Trunks



3 Click the **Add route** button.

The New Route Configuration page appears. See Figure 10 "New Route Configuration".

Figure 10 New Route Configuration


Customer 0, New Route Configuration
- Basic Configuration
Input Description
Input Value
Route Data Block (RDB) (TYPE)
RDB
Customer number (CUST)
0
Route Number (ROUT)
0
Designator field for trunk (DES)
VTRK_H323
Trunk Type (TKTP)
TIE trunk data block (TIE)
Incoming and Outgoing trunk (ICOG)
Incoming and Outgoing (IAO)
Access Code for the trunk route (ACOD)
1000
The route is for a virtual trunk route (VTRK)
- Zone for codec selection and bandwidth management (ZONE)
002
Range: 0 - 255
- Node ID of signaling server of this route (NODE)
9
Range: 0 - 9999
- Protocol ID for the route (PCID)
H323 (H323)
Integrated Services Digital Network option (ISDN)
- Mode of operation (MODE)
Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH)
3
Range: 0 - 254
- Interface type for route (IFC)
Meridian M1 (SL1)
- Private Network Identifier (PNI)
0
Range: 0 - 32700
- Network Calling Name Allowed (NCNA)
- Network Call Redirection (NCRD)
- Recognition of DTI2 ABCD FALT signal for ISL (FALT)
- Channel Type (CHTY)
B-channel (BCH)
- Call Type for outgoing direct dialed TIE route (CTYP)
Coordinated Dialing Plan (CDP)
- Insert ESN Access Code (INAC)
- Integrated Service Access Route (ISAR)

4 Select the **Route Number (ROUT).**

5 For **Designator field for trunk (DES)**, type a meaningful name.

6	For **Trunk Type (TKTP)**, select **TIE Trunk data block (TIE)**.
7	For **Incoming and Outgoing trunk (ICOG)**, select **Incoming and Outgoing (IAO)**.
8	Select the **Access Code for the trunk route (ACOD)**.
9	Select the **The route is for a virtual trunk route (VTRK)** check box.
10	Type the **Zone** number for the new route. This value must match the values you configure in the Signaling Server.
11	Type the **Node ID of signaling server of this route (NODE)**. This value must match the values you configure in the Signaling Server.
12	For **Protocol ID for the route (PCID)**, select **H323**.
13	Select the **Integrated Services Digital Network option (ISDN)** check box.
14	For **Mode of operation (MODE)**, select **Route uses ISDN Signaling Link (ISLD)**.
15	Select the **D-Channel number (DCH)**.
16	For **Interface type for route (IFC)**, select **Meridian M1 (SL1).**
17	Leave the **Call type for outgoing direct dialed TIE route (CTYP)** at the default value. It is best to let NARS/BARS entries determine the NPI/TON for a number so that the route can be used for multiple call types.
18	Select the **Insert ESN Access Code (INAC)** check box.
19	Leave the other default values as is and click **Submit**. The Routes and Trunks screen appears showing the created routes.

End

Creating the virtual trunks (LD 14)

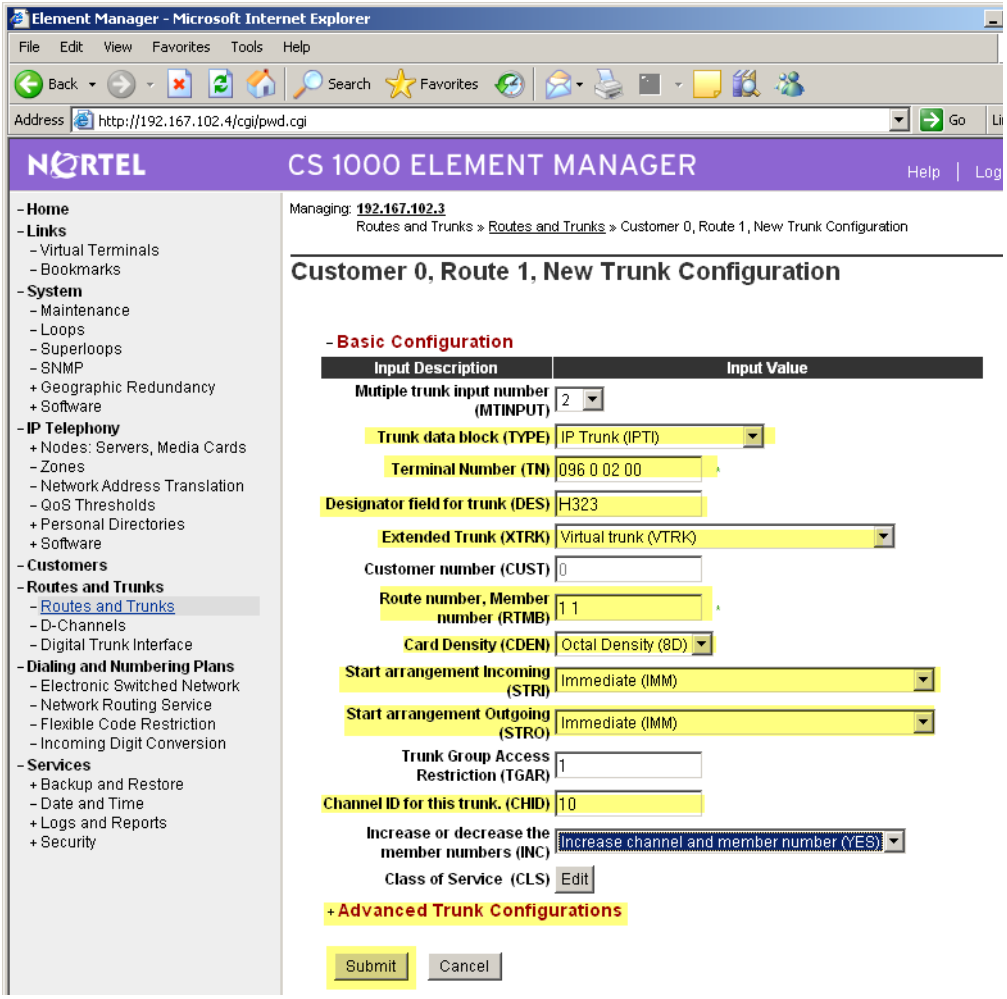
Note: The Virtual Trunk TNs that you configure in this procedure cannot overlap with the ones that you configure for IP phones.

Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > Routes and Trunks**. See Figure 9 "Routes and Trunks" (page 31).
3	Expand the **Customer** heading.
4	Click **Add trunk** next to the route to which you wish to add the trunk.

The New Trunk Configuration page appears. See Figure 11 "New Trunk Configuration".

Note: Create separate virtual routes for SIP and H.323. The SIP route is configured in the section "SIP protocol configuration" (page 43).

Figure 11 New Trunk Configuration



5 If you are configuring several trunks the same way, select the number of the **Multiple trunk input number (MTINPUT)** (optional).

6 For **Trunk data block (TYPE)**, select **IP Trunk (IPTI)**.

7 Type the **Terminal Number (TN)**.

8 For **Designator field for trunk (DES)**, type a meaningful value.

9 For **Extended Trunk (XTRK)**, select **Virtual trunk (VTRK)**.

10 Type the **Route number, Member number (RTMB)**.

11 Set the values of **Start arrangement Incoming (STRI)** and **Start arrangement Outgoing (STRO).**

Immediate (IMM) is recommended for both fields.

12 Select the **Channel ID for this trunk (CHID)**.

Note: You can add a Class of Service (CLS) for all features that you wish. In a basic configuration, you can leave the CLS as is.

13 Select **Advanced Trunk Configurations** to display a list of advanced features.

14 Edit the necessary fields or accept the default values.

15 Click **Submit**.

End

Creating the ESN data block for CDP

Step	Action

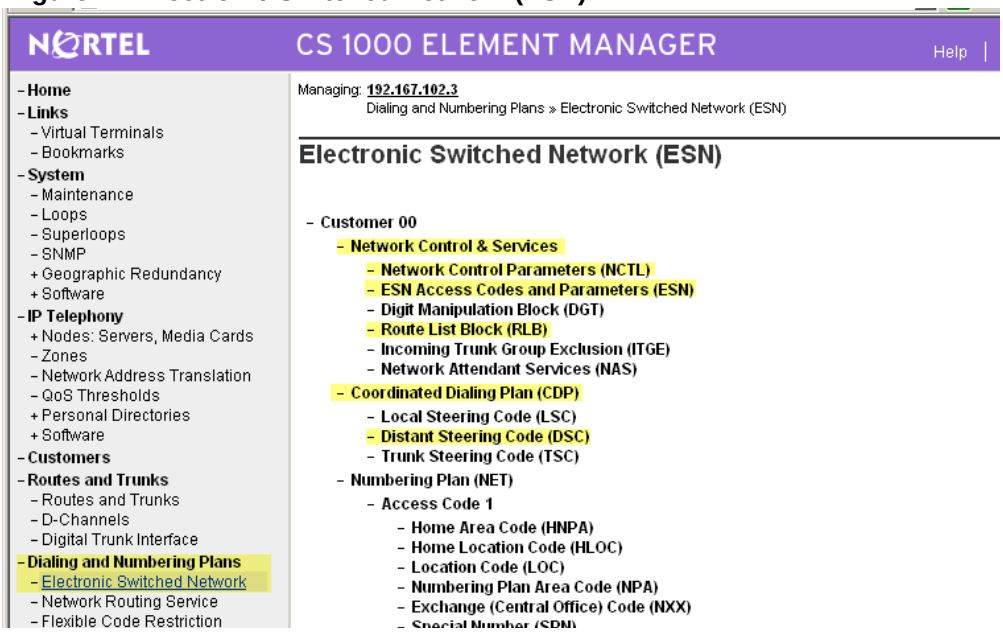
1 Log on to Element Manager.

2 Select **Dialing and Numbering Plans > Electronic Switched Network**.

3 Expand the **Customer** heading.

See Figure 12 "Electronic Switched Network (ESN)".

Figure 12 Electronic Switched Network (ESN)



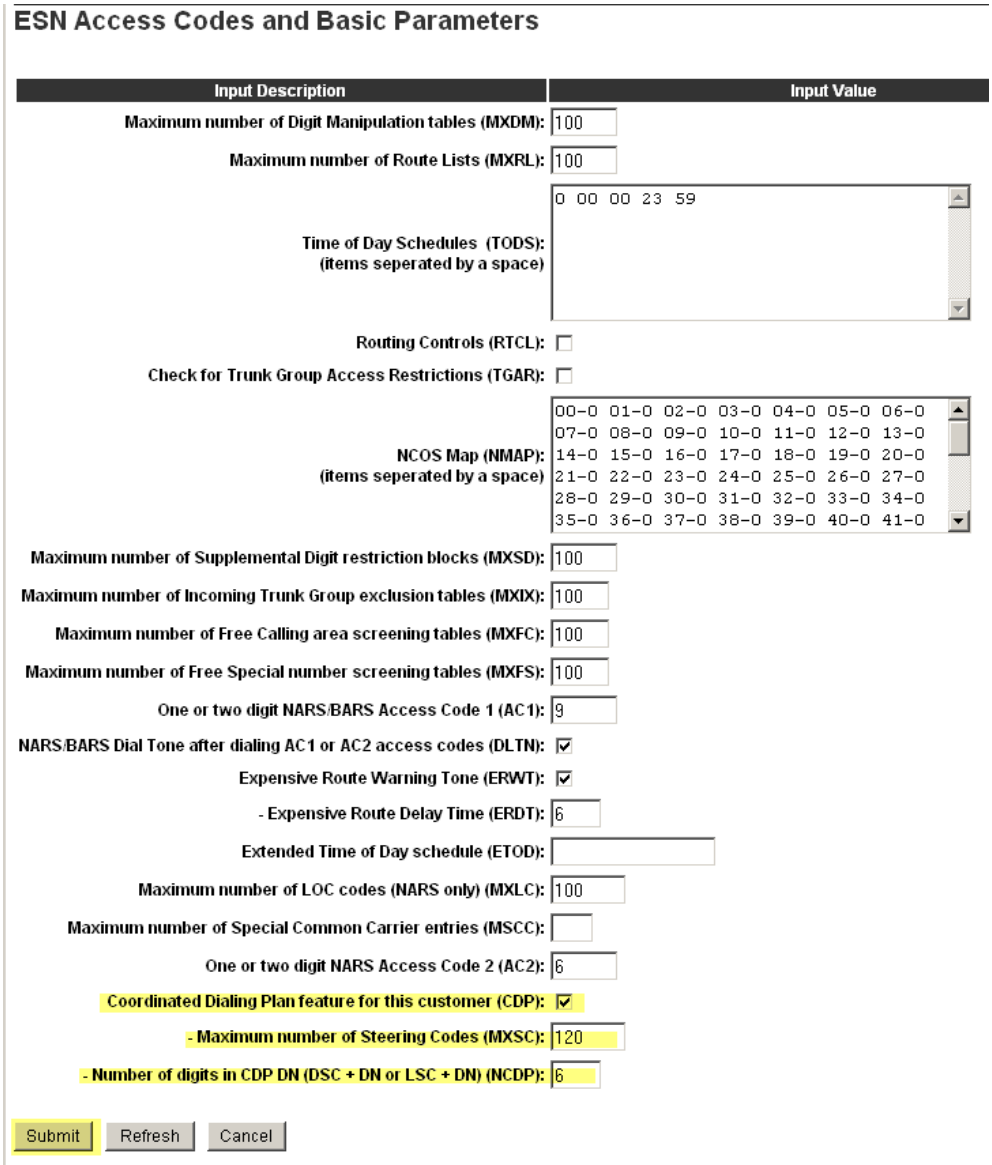
4 Select **Network Control & Services > ESN Access Codes and Parameters (ESN)**.

A message appears if ESN data is not configured. Click **OK**.

The ESN Access Codes and Basic Parameters page appears. See Figure 13 "ESN Access Codes and Basic Parameters".

Note: If ESN data is configured on your switch, the fields on this page appear populated.

Figure 13 ESN Access Codes and Basic Parameters


ESN Access Codes and Basic Parameters
Input Description
Input Value
Maximum number of Digit Manipulation tables (MXDM): 100
Maximum number of Route Lists (MXRL): 100
Time of Day Schedules (TODS): (items seperated by a space)
0 00 00 23 59
Routing Controls (RTCL):
Check for Trunk Group Access Restrictions (TGAR):
NCOS Map (NMAP): (items seperated by a space)
00-0 01-0 02-0 03-0 04-0 05-0 06-0
07-0 08-0 09-0 10-0 11-0 12-0 13-0
14-0 15-0 16-0 17-0 18-0 19-0 20-0
21-0 22-0 23-0 24-0 25-0 26-0 27-0
28-0 29-0 30-0 31-0 32-0 33-0 34-0
35-0 36-0 37-0 38-0 39-0 40-0 41-0
Maximum number of Supplemental Digit restriction blocks (MXSD): 100
Maximum number of Incoming Trunk Group exclusion tables (MXIX): 100
Maximum number of Free Calling area screening tables (MXFC): 100
Maximum number of Free Special number screening tables (MXFS): 100
One or two digit NARS/BARS Access Code 1 (AC1): 9
NARS/BARS Dial Tone after dialing AC1 or AC2 access codes (DLTN):
Expensive Route Warning Tone (ERWT):
- Expensive Route Delay Time (ERDT): 6
Extended Time of Day schedule (ETOD):
Maximum number of LOC codes (NARS only) (MXLC): 100
Maximum number of Special Common Carrier entries (MSCC):
One or two digit NARS Access Code 2 (AC2): 6
Coordinated Dialing Plan feature for this customer (CDP):
- Maximum number of Steering Codes (MXSC): 120
- Number of digits in CDP DN (DSC + DN or LSC + DN) (NCDP): 6
Submit
Refresh
Cancel

5 Edit the main parameters (**MXDM, MXRL, MXSD, MXIX, MXFC, MXFS** and **MXLC)** if required, or leave the default values as is.

6 Select the **Coordinated dialing Plan feature for this customer (CDP)** check box.

7 Set the value of the **Maximum number of Steering Codes (MXSC)**.

8 Set the value of the **Number of digits in CDP DN (DSC+DN or LSC+DN) (NCDP).**

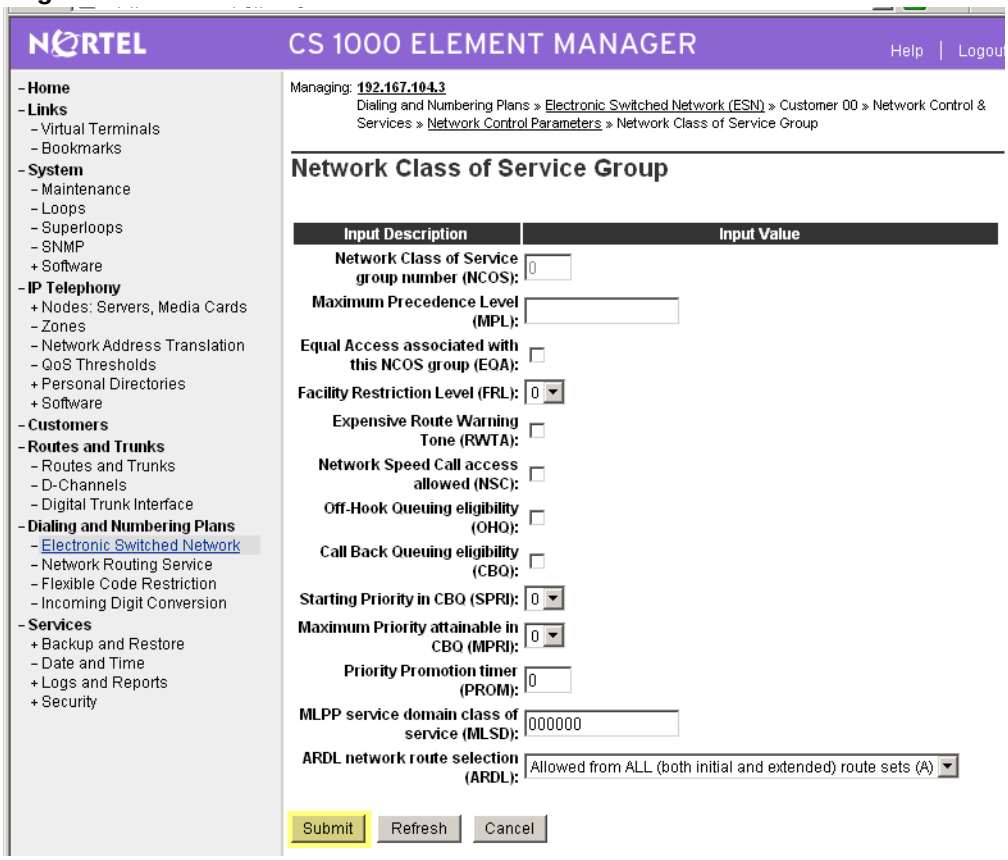
9 Click **Submit**.

End

Creating the Network Control Block (NCTL) for network access (LD 87)

Step	Action
1	Log onto Element Manager.
2	Select **Open Dialing and Numbering Plans > Electronic Switched Networks**.
3	Click the **Customer** tab. See Figure 12 "Electronic Switched Network (ESN)" (page 34).
4	Select **Network Control and Services > Network Class of Service Group Index - x**. A message appears if no network control data is configured. Click **OK** to configure new data.
5	Next to Network Control Basic Parameters, click the **Edit** tab. The Network Control Basic Parameters page appears. See Figure 14 "Network Control Basic Parameters".

Figure 14 Network Control Basic Parameters



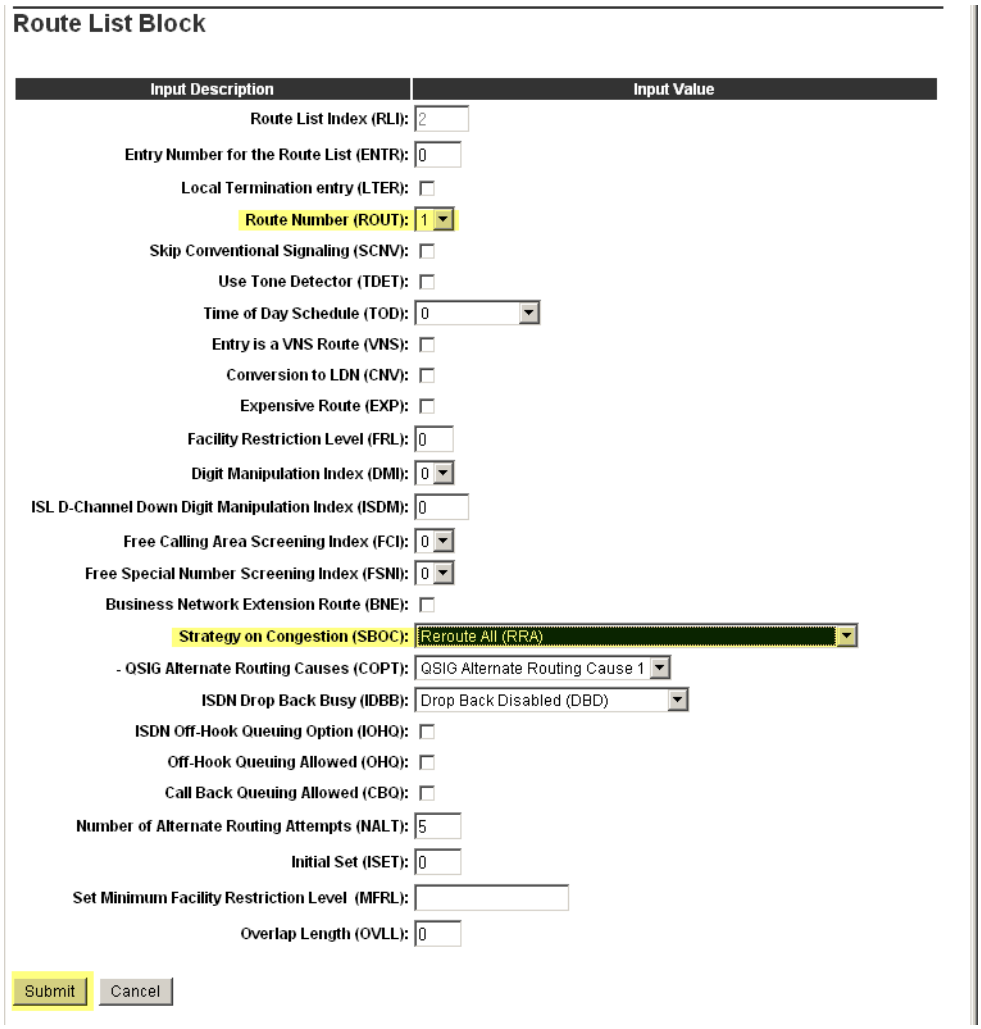
6	If required, type a **Network Class of Service group number (NCOS)**.
7	Click **Submit**.

End

Creating the RLB for the virtual trunk route (LD 86)

Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans > Electronic Switched Networks**.
3	Expand the **Customer** heading. See Figure 12 "Electronic Switched Network (ESN)" (page 34).
4	Select **Network Control and Services > Route List Blocks**. If route list blocks are not configured, the error message “Route List does not exist” appears. Click **OK**.
5	Type the **Route List Index number**.
6	Click **to Add**. The Route List Block Configuration page appears. See Figure 15 "Route List Block".

Figure 15 Route List Block


Route List Block
Input Description
Input Value
Route List Index (RLI): 2
Entry Number for the Route List (ENTR): 0
Local Termination entry (LTER):
Route Number (ROUT): 1
Skip Conventional Signaling (SCNV):
Use Tone Detector (TDET):
Time of Day Schedule (TOD): 0
Entry is a VNS Route (VNS):
Conversion to LDN (CNV):
Expensive Route (EXP):
Facility Restriction Level (FRL): 0
Digit Manipulation Index (DMI): 0
ISL D-Channel Down Digit Manipulation Index (ISDM): 0
Free Calling Area Screening Index (FCI): 0
Free Special Number Screening Index (FSNI): 0
Business Network Extension Route (BNE):
Strategy on Congestion (SBOC): Reroute All (RRA)
- QSIG Alternate Routing Causes (COPT): QSIG Alternate Routing Cause 1
ISDN Drop Back Busy (IDBB): Drop Back Disabled (DBD)
ISDN Off-Hook Queuing Option (IOHQ):
Off-Hook Queuing Allowed (OHQ):
Call Back Queuing Allowed (CBQ):
Number of Alternate Routing Attempts (NALT): 5
Initial Set (ISET): 0
Set Minimum Facility Restriction Level (MFRL):
Overlap Length (OVLL): 0
Submit
Cancel

7 Select the **Route Number (ROUT)** you previously defined.

8 For **Strategy on Congestion (SBOC)**, select **Reroute All (RRA)**.

9 Accept the other defaults and click **Submit**.

The new Route List Block is generated. You can check the configuration by selecting Route List Block Index and Data Entry Index.

End

Creating the CDP steering codes (LD 87)

Step	Action

1 Log on to Element Manager.

2 Select **Dialing and Numbering Plans > Electronic Switched Network**.

3 Expand the **Customer** heading.

See Figure 12 "Electronic Switched Network (ESN)" (page 34).

4 Select **Coordinated Dialing Plan (CDP) > Distant Steering Code List**.

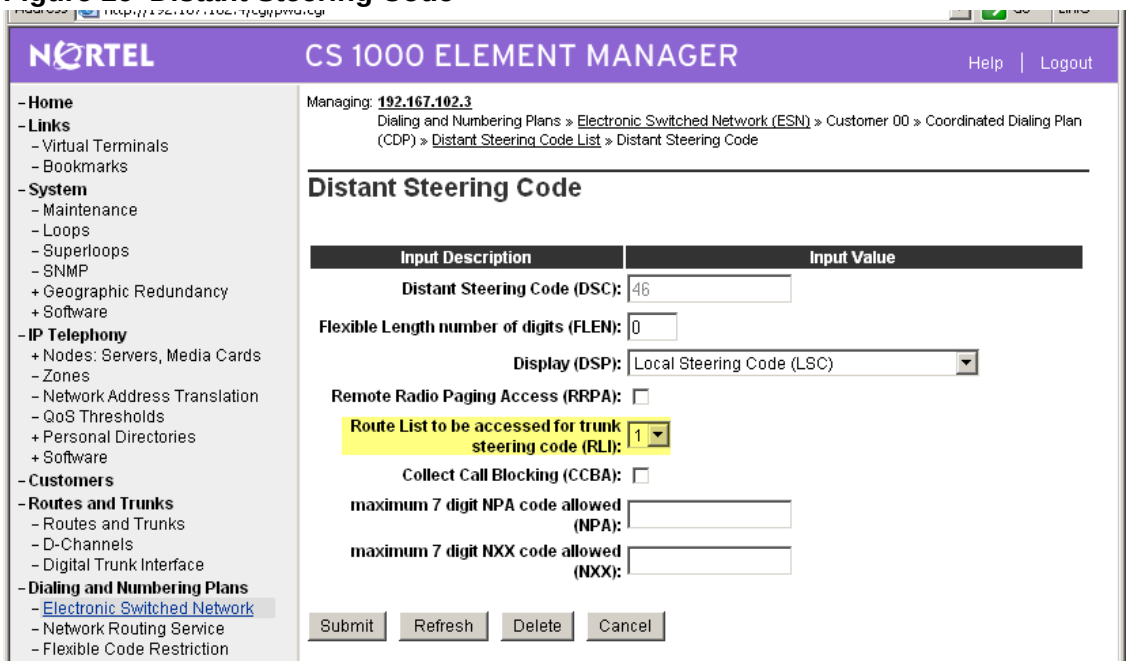
5 Enter the **Distant Steering Code (DSC)**.

This is the DN range of other systems on the network. You can add more steering codes in this manner.

6 Click **to Add**.

The Distant Steering Code page appears. See Figure 16 "Distant Steering Code".

Figure 16 Distant Steering Code



7 Check the populated fields.

8 Select a **Route list to be accessed for trunk steering code (RLI)**.

9 Click **Submit**.

10 Repeat steps 6 to 9 for all other call types on your network:

- LOC (Location Code)
- HLOC (Home Location Code)
- NPA
- HNPA (Home NPA)
- SPN (Special Numbers)
- NXX

This steering code is now defined. You can click the plus sign to view all the entered information.

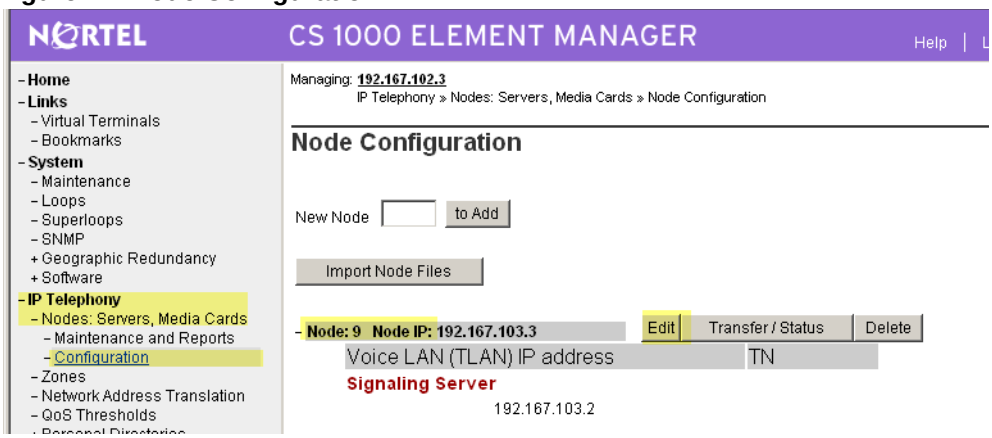
End

Checking CODEC and QoS settings

At this point, the Call Server configuration is complete. It is recommended that you check the CODEC and QoS settings.

Step	Action
1	Log on to Element Manager.
1	Select **IP Telephony Manager > Nodes: Servers, Media Cards > Configuration**. See Figure 17 "Node Configuration".

Figure 17 Node Configuration

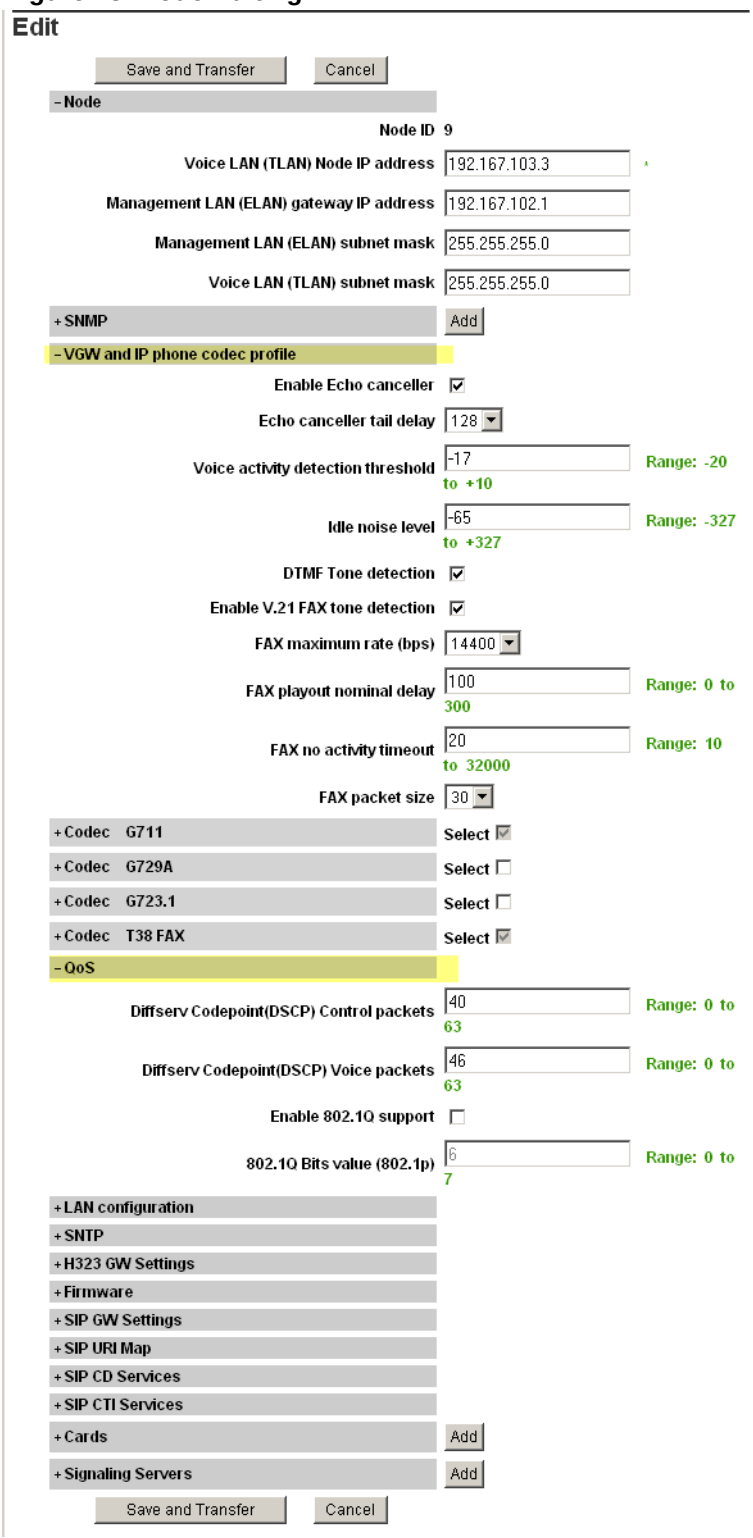


2 Expand the **Node** heading.

3 Click **Edit**.

The Edit page appears. See Figure 18 "Node Editing" (page 40).

Figure 18 Node Editing


Edit
Save and Transfer
Cancel
- Node
Node ID 9
Voice LAN (TLAN) Node IP address 192.167.103.3
Management LAN (ELAN) gateway IP address 192.167.102.1
Management LAN (ELAN) subnet mask 255.255.255.0
Voice LAN (TLAN) subnet mask 255.255.255.0
+ SNMP
Add
- VGW and IP phone codec profile
Enable Echo canceller
Echo canceller tail delay 128
Voice activity detection threshold -17 Range: -20 to +10
Idle noise level -65 Range: -327 to +327
DTMF Tone detection
Enable V.21 FAX tone detection
FAX maximum rate (bps) 14400
FAX playout nominal delay 100 Range: 0 to 300
FAX no activity timeout 20 Range: 10 to 32000
FAX packet size 30
+ Codec G711 Select
+ Codec G729A Select
+ Codec G723.1 Select
+ Codec T38 FAX Select
- QoS
Diffserv Codepoint(DSCP) Control packets 40 Range: 0 to 63
Diffserv Codepoint(DSCP) Voice packets 46 Range: 0 to 63
Enable 802.1Q support
802.1Q Bits value (802.1p) 6 Range: 0 to 7
+ LAN configuration
+ SNTP
+ H323 GW Settings
+ Firmware
+ SIP GW Settings
+ SIP URI Map
+ SIP CD Services
+ SIP CTI Services
+ Cards
Add
+ Signaling Servers
Add
Save and Transfer
Cancel

4 Expand the **VGW and IP phone CODEC profile** heading and edit the fields as necessary.

5 Expand the **QoS** heading and edit the fields as necessary.

6 If you make configuration changes, click **Save and Transfer**; otherwise, click **Cancel**.

End

H.323 Gatekeeper Configuration

Configure the H.323 Gatekeeper in both Element Manager and the NRS. Configure the Element Manager before the NRS.

The sequence of H.323 Gatekeeper configuration procedures is as follows:

- "Configuring Element Manager" (page 41)

Configuring Element Manager

Set the Primary and Alternate Gatekeeper IP addresses. This IP address is configured at each H.323 Gateway (Signaling Server).

1 Log on to Element Manager.

1 Select **IP Telephony Manager > Nodes: Servers, Media Cards > Configuration**.

2 Expand the **Node ID** heading.

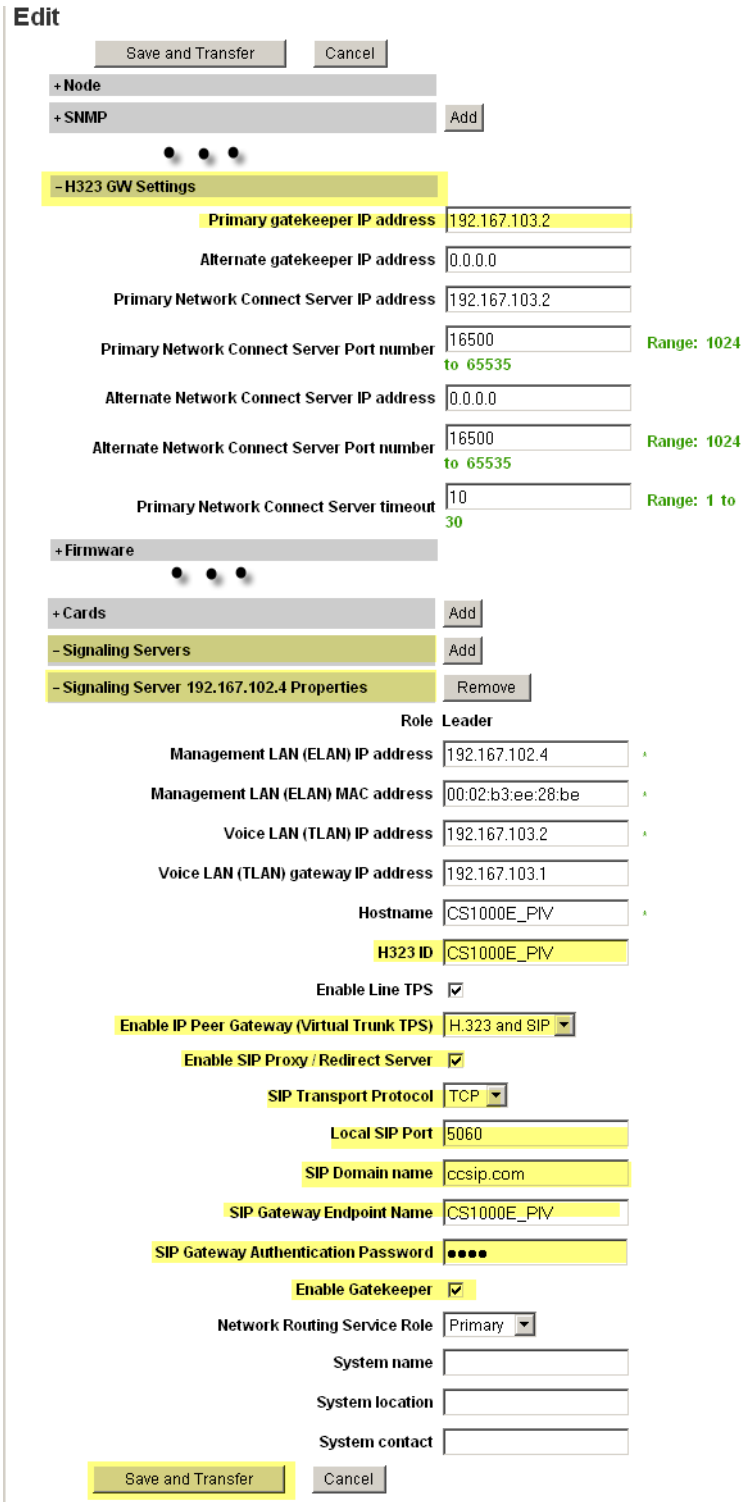
See Figure 17 "Node Configuration" (page 39).

3 Click **Edit**.

4 Expand the **H.323 GW Settings** heading.

See Figure 19 "H323 Gateway and Signaling Server" (page 42).

Figure 19 H323 Gateway and Signaling Server



5 Enter the **Primary Gatekeeper IP address**.

This is the T-LAN IP address of the Signaling Server that runs the Gatekeeper application. This is not the same as the Node IP.

6 Enter the **Alternate Gatekeeper IP address** if you have an alternate on your system (optional).

7 Expand the **Signaling Servers** heading.

8 Expand the **Signaling Server Properties** heading.

9 Enter the **H323 ID**.

This should be the same as the Signaling Server that hosts the Primary H.323 Gatekeeper. Make a note of the H323 ID for the NRS configuration.

Note: The host name does not need to be the same as the H323 ID, but it is recommended that both names are the same.

10 Select the **Enable Gatekeeper** check box.

11 Click **Save and Transfer**.

End

SIP protocol configuration

SIP addressing and Universal Resource Identifier

SIP addressing is built around either a telephone or a Web host name. For example, the SIP address can be based on a URL such as SIP:john.doe@companyabc.com. This URL is part of the Universal Resource Identifier (URI), which is used for SIP address resolution.

The user ID shows the composition of a SIP address. The SIP configuration of the Redirect Server is based on this address. The Domain name is the main address of a SIP server; you can compare it to a node ID. This is also the Service Domain that you enter in the NRS.

At the end of the URI, the user=phone section shows that this is the URI for a telephone user.

In SIP address resolution, the user-name field is parsed into name and phone context. Address lookup is based on digits, phone context, and domain name. This means that the telephone number undergoes SIP mapping. The Service Domain is divided into Level 0 (L0) and Level 1 (L1) domains. These domains are entered in the NRS.

SIP Gateway URI mapping and addressing

The SIP Gateway on the NRS provides the CS 1000 system with a direct trunking interface between the CS 1000 systems and a SIP domain.

The SIP Gateway has the following features:

- SIP User Agent (UA), which services one or more end-users in making/receiving SIP calls
- Signaling Gateway for all CS 1000 telephones (analog, digital, and IP Phones), which maps ISDN messages to and from SIP messages
- H.323 Gateway functionality
- MCDN, MWI partially mapped (mainly name display), partially tunneled
- ESN5, EPID tunneled

The SIP Gateway has the following functions:

- maps telephony numbers to and from SIP Uniform Resource Identifiers (URIs)
- performs client registration

- maps ISDN messages to and from SIP messages
- sets up the speech path between the desktop and SIP endpoints
- uses a standard SIP authentication security mechanism

Note: The private numbering plans, public/unknown numbers and public/special numbers also have explicit one-to-one mappings to SIP URI. They must be defined by preconfigured subdomain names. You must define the subdomain name on both the Gateway and proxy/registrar.

Configuration for the SIP protocol

Configuration for the SIP protocol is very similar to that of the Call Server.

The basic configuration for IP Peer Networking for SIP is performed in the following order:

1 Call Server in Element Manager:

2 SIP Gateway

3 SIP Redirect Server and URI Map

4 Call Server

5 Network Routing Service in the NRS Manager

6 SIP addressing

7 SIP Virtual Trunking

Note: If you select YES at the CRID prompt, a new line (SIP message) is added to the end of the Call Detail Record. This message shows the SIP addressing scheme.

Tip: The SIP Gateway also supports H.323 Gateway functionality so that both Gateways can interoperate. Also, you can point the virtual trunks, whether they are H.323 or SIP, to the same node ID on the signaling server. Then, the signaling server can perform the signaling for both protocols.

The procedures in this section are as follows:

— "Enabling the SIP Virtual Trunk application" (page 45)
— "Configuring the SIP Gateway" (page 45)
— "Configuring the SIP Redirect Server and URI map" (page 47)
— "Configuring IP networking for SIP" (page 48)
— "Defining the customer to support ISDN " (page 48)
— "Creating the virtual D-channel" (page 48)
— "Configuring the zones in LD 117" (page 49)
— "Creating the virtual route (LD 16)" (page 30)
— "Creating the virtual trunks (LD 14)" (page 52)
— "Creating the ESN data block for CDP" (page 54)
— "Creating the Network Control Block (NCTL) for network access (LD 87)" (page 55)

— "Creating the RLB for the virtual trunk route (LD 86)" (page 55)

— "Creating the CDP steering codes (LD 87)" (page 56)

— "Checking CODEC and QoS settings" (page 57)

Enabling the SIP Virtual Trunk application

Enable SIP functionality in Element Manager.

Step	Action
1	Log on to Element Manager.
2	Select **IP Telephony > Nodes: Servers, Media Cards > Configuration**. See Figure 17 "Node Configuration" (page 39).
3	Expand the **Node** heading.
4	Click **Edit**.
5	Expand the **Signaling Servers** heading.
6	Expand the **Signaling Server Properties** heading. See Figure 19 "H323 Gateway and Signaling Server" (page 42).
7	Select a SIP option (**SIP only** or **H.323 and SIP**) for **Enable IP Peer Gateway (Virtual Trunk TPS)**.
8	Select the **Enable SIP Proxy/Redirect Server** check box.
9	Select the **SIP Transport Protocol**. TCP is the default. UDP means User Datagram Protocol in this instance.
10	Verify the **Local SIP Port**. The default is 5060.
11	Enter the **SIP Domain Name**. The SIP Domain Name must be less than 128 characters in length. Valid characters are a-z, 0-9, period, hyphen, comma, and underscore. This string builds all SIP messages and appears in the URI phone context. If you enable the SIP Gateway application, specify this field. This name must match the Service Domain name configured in NRS.
12	Enter the **SIP Gateway Endpoint Name** and **Authentication Password**. These must match the user ID and password for NRS. This user ID and password helps authenticate the Gateway with the MCS5100 Proxy Server, if you configure Converged Desktop.
13	Click **Save and Transfer**.
	End

Configuring the SIP Gateway

Before you configure the SIP Gateway, check which route you have configured as a SIP route in LD 16. You must fill in this route later.

1 Log on to Element Manager.

2 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration**.

See Figure 17 "Node Configuration" (page 39).

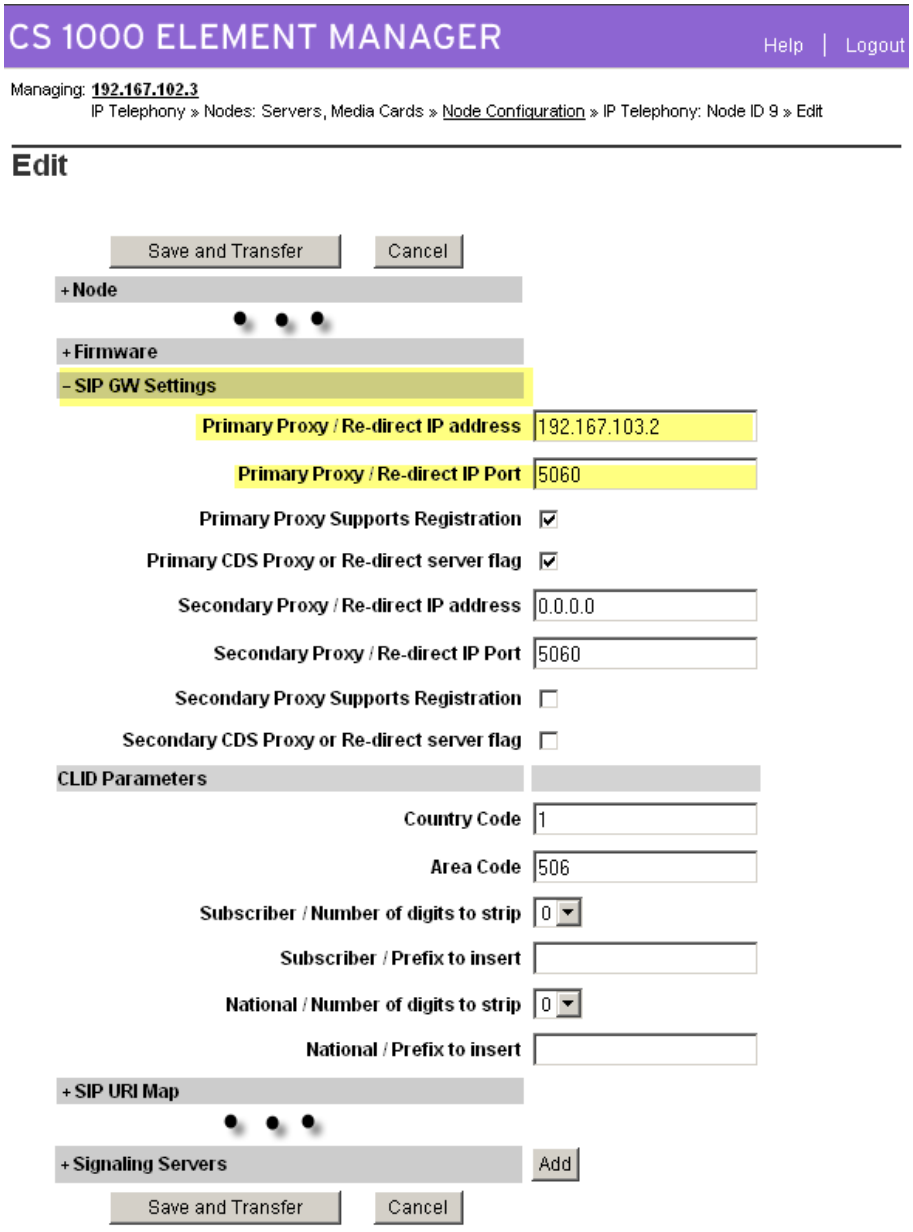
3 Select the **Node**.

4 Click **Edit**.

5 Expand the **SIP GW Settings** heading.

See Figure 20 "Edit SIP GW settings".

Figure 20 Edit SIP GW settings



6 For the **Primary Proxy/Re-direct IP address**, type the T-LAN IP address of the Signaling Server that houses the Redirect Server.

7 For **Primary Proxy/Re-direct IP Port**, use the default port value of 5060.

Note: You can use the T-LAN IP Address of the Alternate NRS in the Secondary Proxy/Re-direct IP address field.

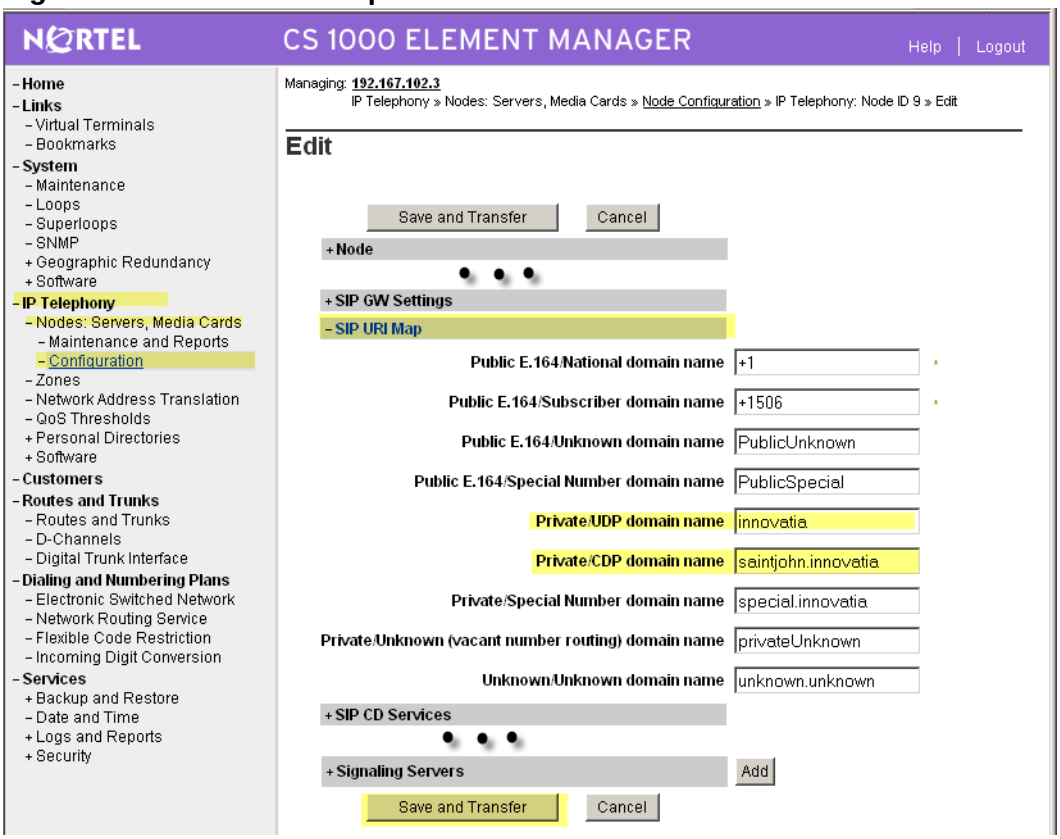
End

Configuring the SIP Redirect Server and URI map

Use this procedure to configure your SIP numbering plan mapping. You can use this mapping to interpret TON/NPI numbers and map them to the associated context (to or from SIP). The TON/NPI field explicitly maps to the SIP phone-context attribute in the URI address.

Step	Action
1	Log on to Element Manager.
2	Select **IP telephony > Configuration**.
3	Expand the **SIP URI Map** heading. See Figure 21 "Edit SIP URI Map".

Figure 21 Edit SIP URI Map



4 In the **Private/UDP domain name** field, type the L1 domain.

5 In the **Private/CDP domain name** field, type the L0 and L1 domains in the format <L0 domain.L1 domain>.

6 Enter the values for your SIP numbering plan in the appropriate fields.

7 Click **Save and Transfer**.

8 Reboot the Signaling Server for the changes to take effect.

End

Configuring IP networking for SIP

The IP Peer Networking configuration for SIP in the Call Server is similar to the H.323 configuration. Complete the following steps for each Call Server in the IP Peer Network:

1. Define the Customer to support ISDN (LD 15).
2. Create the Virtual D-Channel (LD 17).
3. Configure the Zones (LD 117).
4. Create the Virtual Route (LD 16).

   Enter SIP in the VTRK screen.
5. Create the Virtual Trunk.
6. Create the ESN Data Block for CDP (LD 86).
7. Create the Network Control (NCTL) Block for Network Access (LD 87).
8. Create the RLB that uses the Virtual Trunk Route (LD 86).
9. Create the CDP Steering Codes (LD 87).

Note: If the system is configured for H.323, you do not need to configure steps 1, 2, 3, 6, and 7 again.

Defining the customer to support ISDN

Step	Action
1	Log on to Element Manager.
2	Select **Customers**. See Figure 3 "Customers" (page 25).
3	Click **Edit**. A list of enabled feature packages appears.
4	Scroll down and select **ISDN and ESN Networking Package 145**.
5	Select the **Integrated Services Digital Network (ISDN)** check box.
6	Click **Submit**.

End

Creating the virtual D-channel

Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > D-Channels**.

The D-Channels page appears. See Figure 5 "D-Channels" (page 27).

Note: If a D-Channel is not configured, the following message appears: Do not have any D-Channel configured in the system! To add a new D-Channel, click on [OK]. [H0046]

3 From the **Choose a D-Channel Number** menu, select the D-Channel number.

4 From the **Type** menu, select the D-Channel type.

5 Click **to Add**.

The D-Channels Property Configuration page appears. See Figure 6 "D-Channels Property Configuration" (page 28).

6 For the **D Channel Card Type (CTYP)**, select **D-channel is over IP (DCIP)**.

7 For the **Designator (DES)**, type a meaningful name.

The Designator cannot contain spaces; use underscores instead.

Make a note of the Designator in your records for future reference.

8 For **User (USR)**, select **Integrated Services Signaling Link Dedicated (ISLD)**.

9 For **Interface type for D-channel (IFC)**, select **Meridian Meridian1 (SL1)**.

10 Leave all other parameters as is and click **Submit**.

The new channel appears.

End

Configuring the zones in LD 117

Before you can configure the virtual routes and trunks, configure the following zones, in any order:

- Zone 1 = IP Phones zone (ZBRN = MO)
- Zone 2 = Voice Gateway Channels zone, which should be different from the IP Phones zone (ZBRN = VTRK)

Ensure that enough bandwidth is allocated for the zones with the heaviest traffic.

Step	Action

1 Log on to Element Manager.

2 Select **IP Telephony > Zones**.

See Figure 7 "Zones" (page 29).

3 Select **Zone 1**.

Note: If Zone 1 is configured, it appears in the list of configured zones at the bottom of the page.

4 Click **to Add**.

The Zone Basic Property and Bandwidth Management page appears. See Figure 8 "Zone Basic Property and Bandwidth Management" (page 30).

Note: The following message can appear after you click **to Add**:

To maintain consistent zone properties within the network, it is recommended to use the “Zone Basic Property and Bandwidth Management Spreadsheet”. Do you wish to proceed?

Click the **OK** button.

5 Leave the default values for bandwidth and resource type as is.

6 Set the **Zone Intent (ZBRN)** as follows:

- Zone 1 is for the IP Phones at the Main Office. Set Zone Intent (ZBRN) for Zone 1 to **MO**.
- Zone 2 is for the Voice Gateway Channels. Set Zone Intent (ZBRN) for Zone 2 to **VTRK**.

7 For **Description (ZDES)**, type a meaningful description.

8 Click **Submit**.

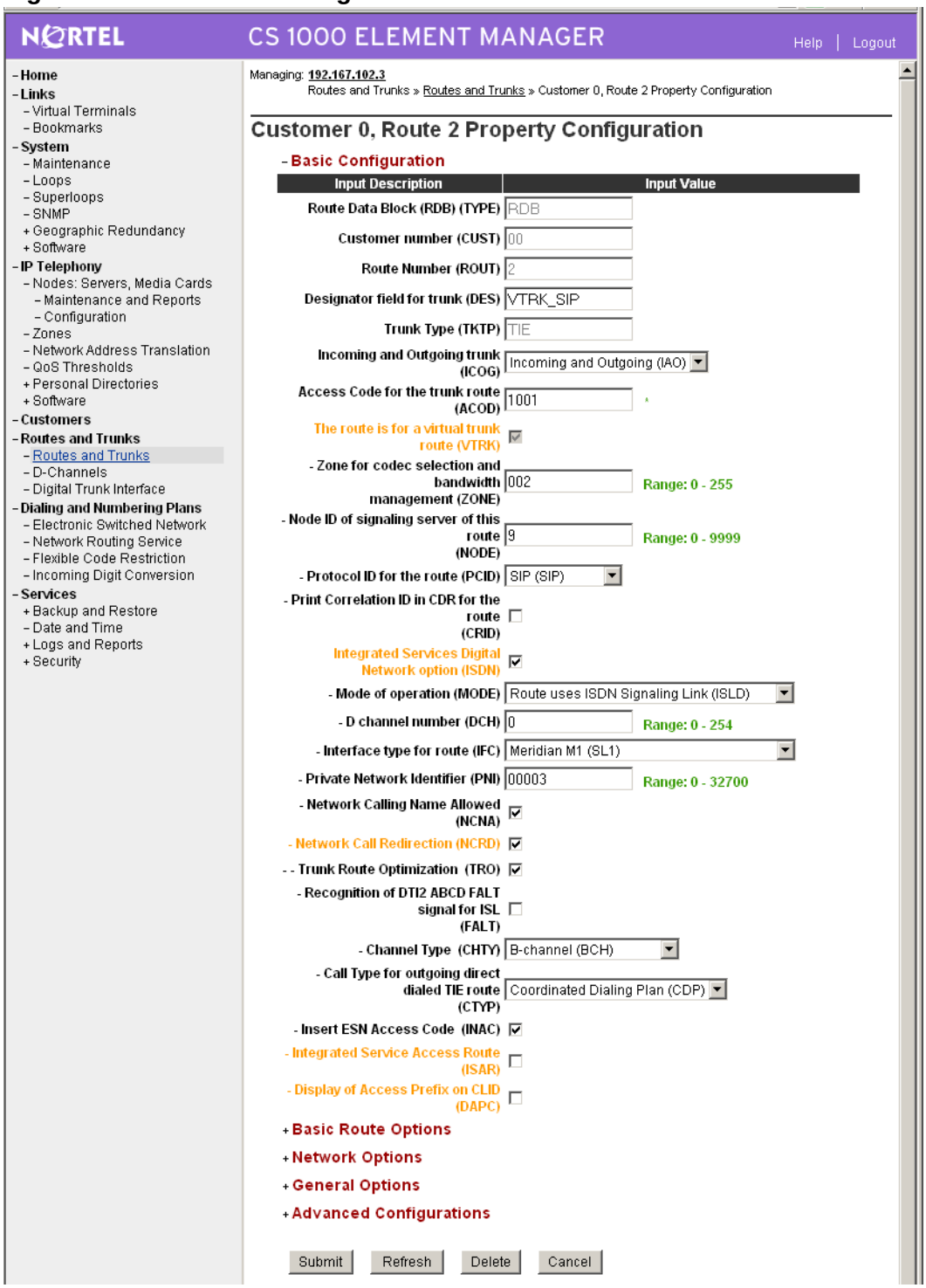
9 Repeat for Zones 2 and 3.

End

Creating the virtual route (LD 16)

Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > Routes and Trunks**.
3	Expand the **Customer** heading. See Figure 9 "Routes and Trunks" (page 31).
4	Click the **Add route** button. The New Route Configuration page appears. See Figure 22 "New Route Configuration" (page 51).

Figure 22 New Route Configuration



5 Enter a virtual **Route number (ROUT)**.

6 Enter a **Designator field for trunk (DES)**, for example, DEV_VTRK_2.

7 For **Trunk Type (TKYP)**, select **TIE Trunk data block (TIE)**.

8 For **Incoming and Outgoing Trunk (ICOG)**, select Incoming and Outgoing (IAO).

9 For **Access Code for the trunk route (ACOD)**, select an unused number.

10 Select the **Route is for a virtual trunk route (VTRK)** check box.

11 Enter the **zone number** and **Node ID**.

Make sure these numbers are the same ones you configure in the Signaling Server.

12 Confirm that the **Protocol ID** is set to **SIP**.

13 Select the **ISDN** check box.

14 For **Mode of Operation (MODE)**, select **Route uses ISDN Signaling Link (ISLD)**.

15 Enter the **D-Channel number**.

16 For **Interface type for route (IFC)**, select **Meridian M1 (SL1)**.

17 Leave the **Call type for outgoing direct dialed TIE route (CTYP)** at the default value.

It is best to let NARS/BARS entries determine the NPI/TON for a number so that the route can be used for multiple call types.

18 Select the **INAC** check box.

19 Accept all other default values and click **Submit**.

The Routes and Trunks page appears, showing both routes.

End

Creating the virtual trunks (LD 14)

Step	Action

1 Log on to Element Manager.

2 Select **Routes and Trunks > Routes and Trunks**.

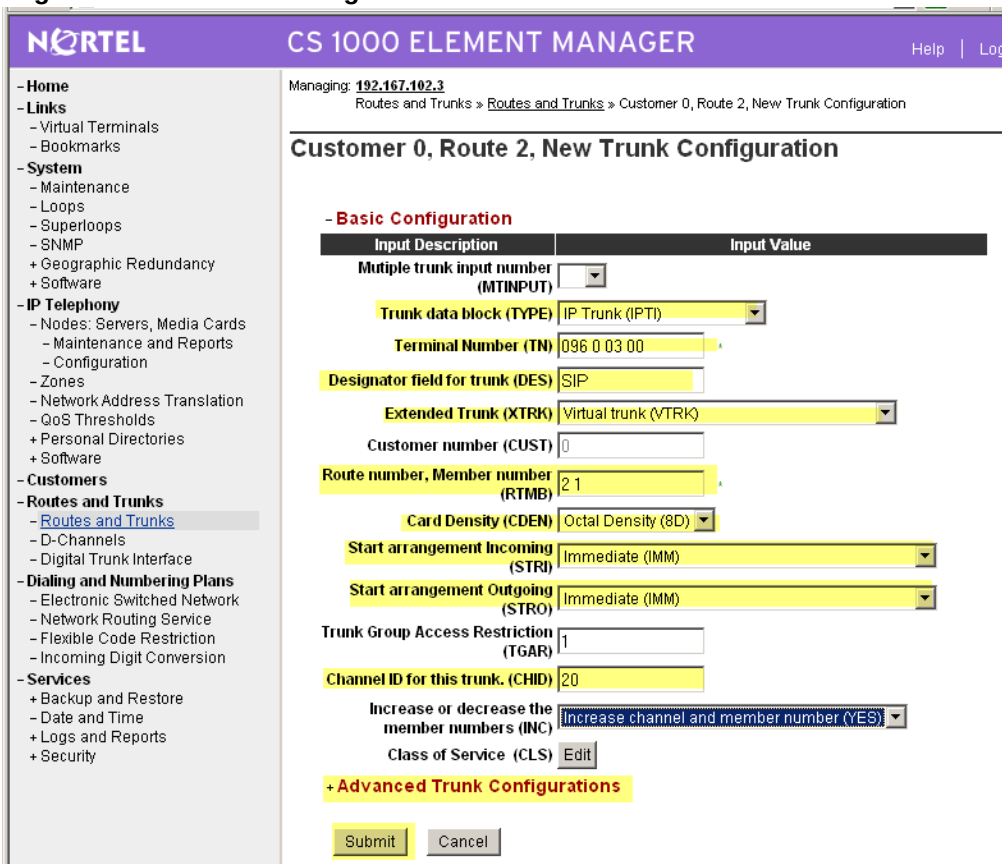
3 Expand the **Customer** heading.

4 Click **Add trunk** next to the desired route.

The New Trunk Configuration page appears. See Figure 23 "New trunk configuration" (page 53).

Note: Create separate virtual routes for SIP and H.323. The H.323 route is configured in "Creating the virtual trunks (LD 14)" (page 32).

Figure 23 New trunk configuration



5 Select a **Multiple trunk input number (MTINPUT)** (optional).

6 For **Trunk data block (TYPE)**, select **IP trunk (IPTI)**.

7 Type a virtual **Terminal Number (TN)** (for example, 81 0).

8 Type a **Designator field for trunk (DES)**.

9 For **Extended Trunk (XTRK)**, select **VTRK**.

10 Type a **Route number, Member number (RTMB)**.

11 Set **Start arrangement Incoming (STRI)**.

Immediate (IMM) is recommended.

12 Set **Start arrangement Outgoing (STRO)**.

Immediate (IMM) is recommended.

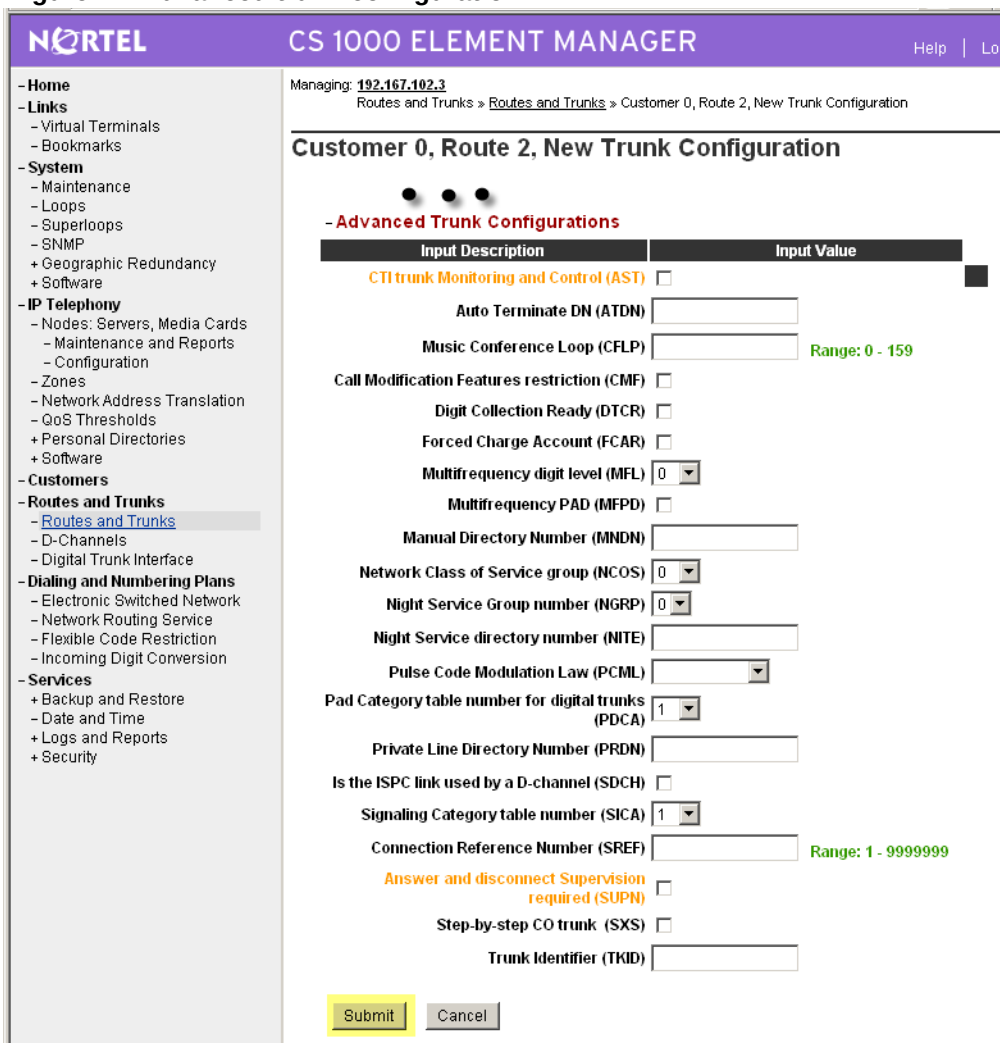
13 Select the **Channel ID for this trunk (CHID)**.

Note: You can add a Class of Service (CLS) for all features. In a basic configuration, you can leave CLS as is.

14 Select **Advanced Trunk Configurations**.

See Figure 24 "Advanced trunk configuration" (page 54).

Figure 24 Advanced trunk configuration



15 Accept the default parameters, or edit them if required.

16 Click **Submit**.

End

Creating the ESN data block for CDP

Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans > Electronic Switched Network**.
3	Expand the **Customer** heading. See Figure 12 "Electronic Switched Network (ESN)" (page 34).
4	Select **Network Control & Services > ESN Access Codes and Parameters (ESN)**.
5	A message appears if no ESN data is configured. Click **OK**.

The ESN Access Codes and Basic Parameters page appears. See Figure 13 "ESN Access Codes and Basic Parameters" (page 35).

Note: If ESN data is configured on your switch, the fields on this page appear populated.

6 Edit the main parameters (**MXDM, MXRL, MXSD, MXIX, MXFC, MXFS** and **MXLC)** if required, or leave the default values as is.

7 Select the **Coordinated dialing Plan feature for this customer (CDP)** check box.

8 Set the value of the **Maximum number of Steering Codes (MXSC)**.

9 Set the value of the **Number of digits in CDP DN (DSC+DN or LSC+DN) (NCDP).**

10 Click **Submit**.

End

Creating the Network Control Block (NCTL) for network access (LD 87)

Step	Action
1	Log onto Element Manager.
2	Select **Open Dialing and Numbering Plans > Electronic Switched Networks**.
3	Click the **Customer** tab. See Figure 12 "Electronic Switched Network (ESN)" (page 34).
4	Select **Network Control and Services > Network Class of Service Group Index - x**. A message appears if no network control data is configured. Click **OK** to configure new data.
5	Next to Network Control Basic Parameters, click the **Edit** tab. The Network Control Basic Parameters page appears. See Figure 14 "Network Control Basic Parameters" (page 36).
6	If required, type a **Network Class of Service group number (NCOS)**.
7	Click **Submit**.

End

Creating the RLB for the virtual trunk route (LD 86)

Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans > Electronic Switched Networks**.
3	Expand the **Customer** heading.

See Figure 12 "Electronic Switched Network (ESN)" (page 34).

4 Select **Network Control and Services > Route List Blocks**.

If route list blocks are not configured, the error message “Route List does not exist” appears. Click **OK**.

5 Type the **Route List Index number**.

6 Click **to Add**.

The Route List Block Configuration page appears. See Figure 15 "Route List Block" (page 37).

7 Select the **Route Number (ROUT)** you previously defined.

8 For **Strategy on Congestion (SBOC)**, select **Reroute All (RRA)**.

9 Accept the other defaults and click **Submit**.

The new Route List Block is generated. You can check the configuration by selecting **Route List Block Index and Data Entry Index**.

End

Creating the CDP steering codes (LD 87)

Step	Action

1 Log on to Element Manager.

2 Select **Dialing and Numbering Plans > Electronic Switched Network**.

3 Expand the **Customer** heading.

See Figure 12 "Electronic Switched Network (ESN)" (page 34).

4 Select **Coordinated Dialing Plan (CDP) > Distant Steering Code List**.

5 Enter the **Distant Steering Code (DSC)**.

This is the DN range of other systems on the network. You can add more steering codes in this manner.

6 Click **to Add**.

The Distant Steering Code page appears. See Figure 16 "Distant Steering Code" (page 38).

7 Check the populated fields.

8 Select a **Route list to be accessed for trunk steering code (RLI)**.

9 Click **Submit**.

10 Repeat steps 6 to 9 for all other call types on your network:

- LOC (Location Code)
- HLOC (Home Location Code)
- NPA
- HNPA (Home NPA)
- SPN (Special Numbers)
- NXX

This steering code is now defined. You can click the plus sign to view all the entered information.

End

Checking CODEC and QoS settings

At this point, the Call Server configuration is complete. It is recommended that you check the CODEC and QoS settings at this point.

1 Log on to Element Manager.

1 Select **IP telephony Manager > Nodes >Node configuration**.

2 Expand the **IP Telephone : Node ID** heading.

3 Click **Edit**.

The Node Information page appears. See Figure 18 "Node Editing" (page 40).

4 Click **VGW and IP phone CODEC profile**.

5 Click **QoS**.

6 If changes are required, make the changes and click **Save and Transfer**.

OR

If the information is configured correctly, click **Cancel**.

NRS configuration

The Network Routing Service (NRS) uses a basic SIP structure for its configuration, which is applicable for SIP, H.323, and Network Connection Server (NCS) call completion. This structure is the basis of the single network dialing/numbering plan.

Before you begin configuration of the NRS, have the names of all domains and subdomains.

NRS configuration procedures

The sequence of NRS configuration procedures is as follows:

- "Enabling NRS" (page 59)
- "Launching NRS Manager" (page 61)
- "Verifying and adjusting system-wide settings" (page 62)
- "Configuring the NRS server settings (H.323 Gatekeeper or SIP)" (page 64)
- "Configuring the service domain" (page 66)
- "Configuring the L1 domain (UDP)" (page 67)
- "Configuring the L0 domain (CDP)" (page 70)
- "Configuring Gateway endpoints" (page 74)
- "Configuring routing entries" (page 78)
- "Configuring collaborative servers" (page 80)
- "Updating the database" (page 81)
- "Checking the status of registered endpoints" (page 82)
- "Performing an H.323 routing test" (page 83)
- "Checking the status of virtual D-channels" (page 84)
- "Checking the status of virtual trunks" (page 85)
- "Committing Gatekeeper configuration changes" (page 86)

Enabling NRS

Step	Action
1	Log on to Element Manager.
2	Select **IP Telephony > Nodes: Servers, Media Cards > Configuration**.
3	Click **Edit**.

4 Scroll to the bottom of the page and select **Signaling Servers**.

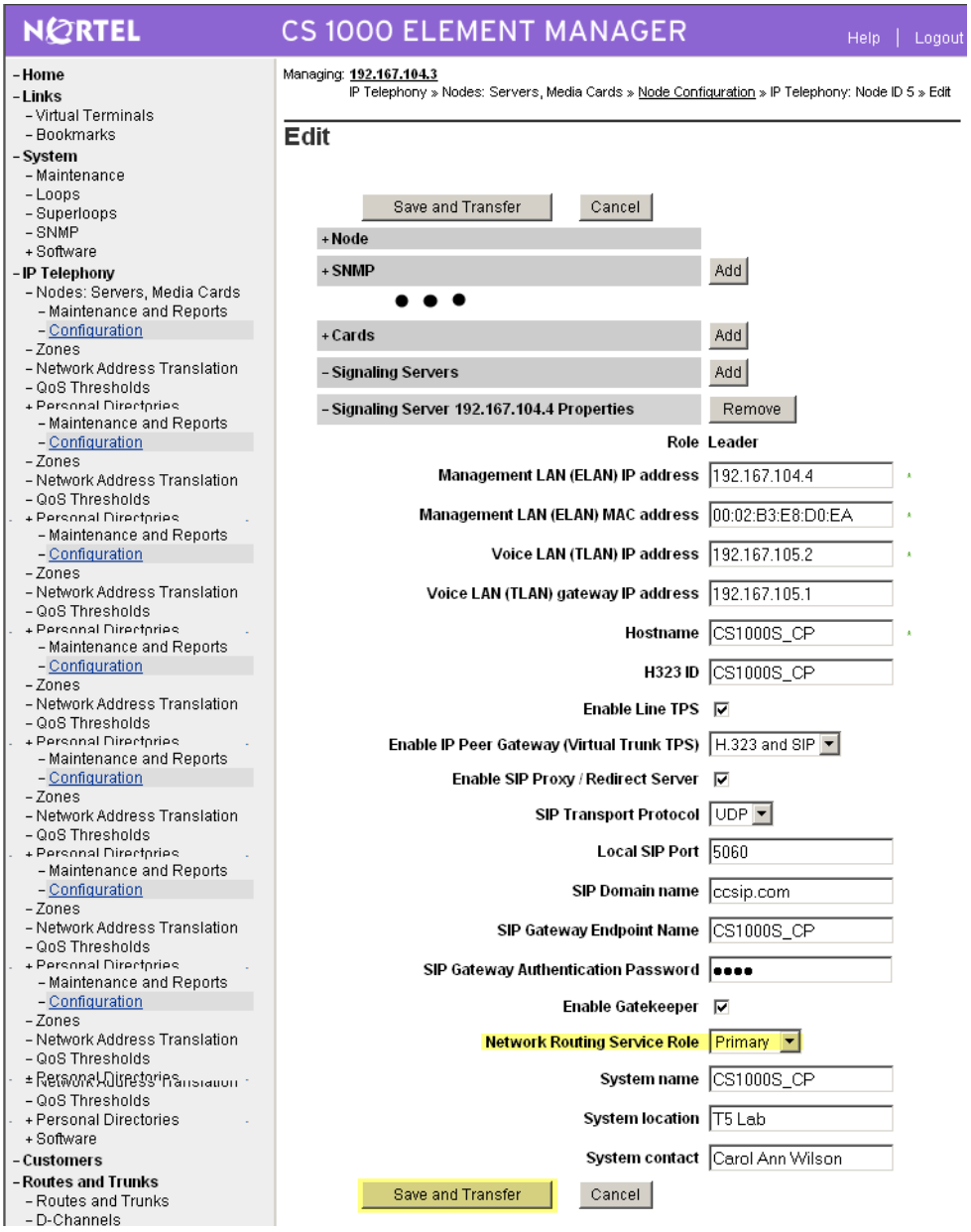
5 Select the **Signaling Server** where you want to install NRS.

Your Signaling Server configuration appears. See Figure 25 "Signaling Server".

6 In the **Network Routing Service Role** field, select **Primary, Alternate or Failsafe**.

7 Click **Save and Transfer**.

Figure 25 Signaling Server

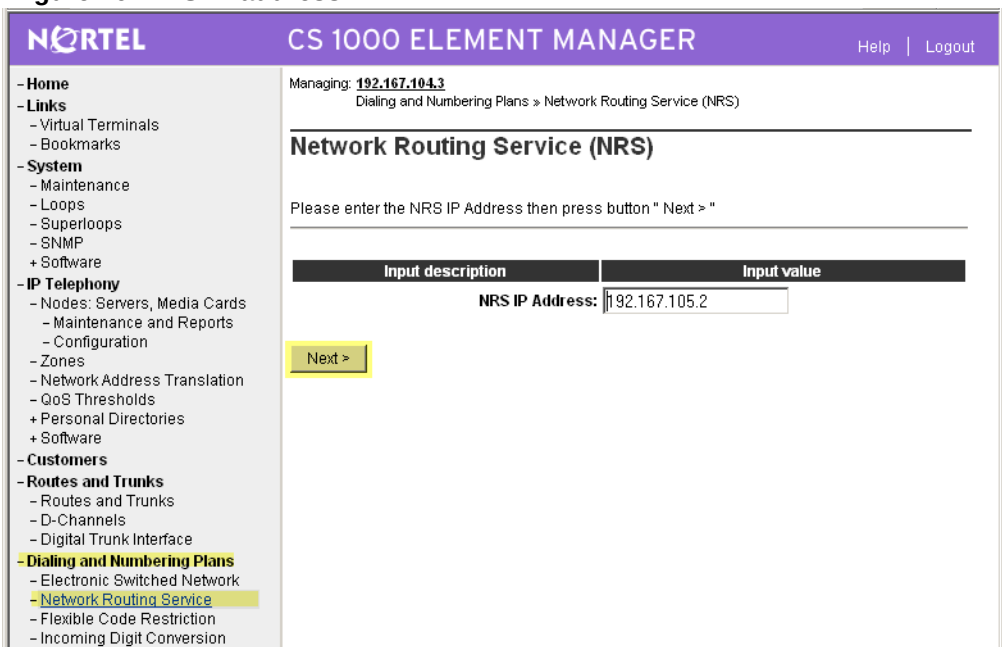


End

Launching NRS Manager

Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans**.
3	Select **Network Routing Service**. The NRS IP address autopopulates in a browser. See Figure 26 "NRS IP address".

Figure 26 NRS IP address

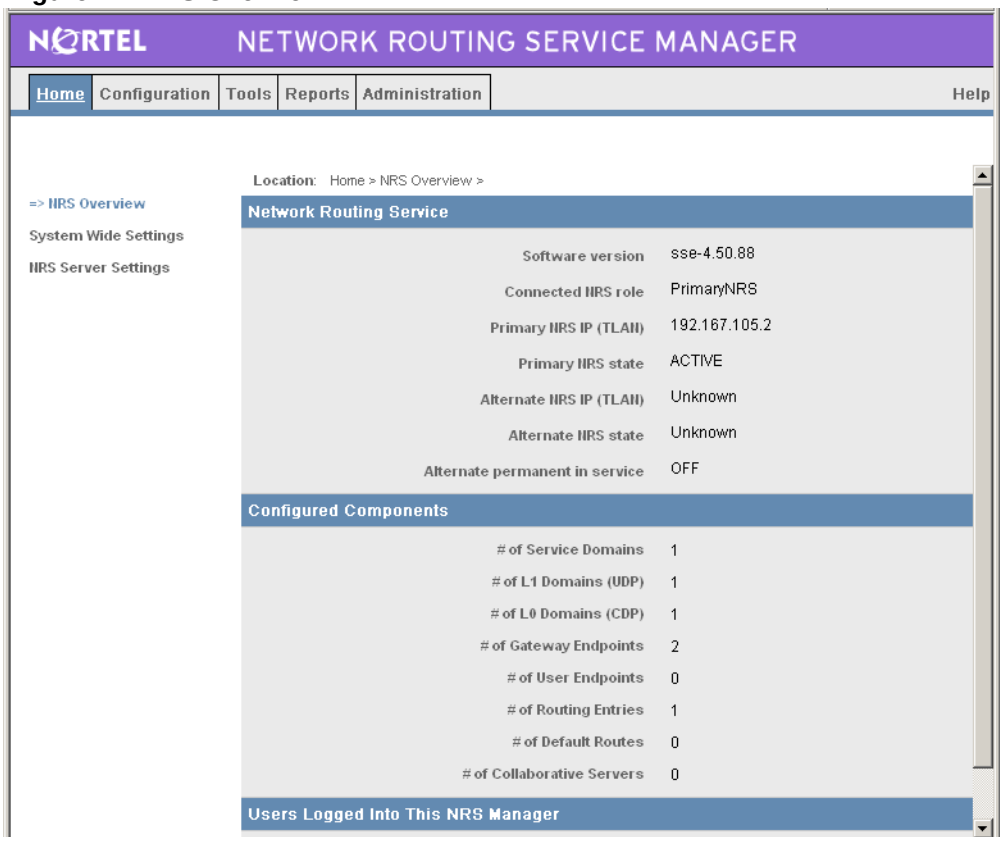


Step	Action
4	Click **Next**. The NRS logon page appears.

Note: To access the Signaling Server, open a Web browser and enter the Node IP address/NRS in the address line. This opens the NRS logon page.

Step	Action
5	Type **admin** for both your default user ID and password. You can change your user ID and password later if necessary. The NRS Overview page appears. See Figure 27 "NRS Overview" (page 62).

Figure 27 NRS Overview



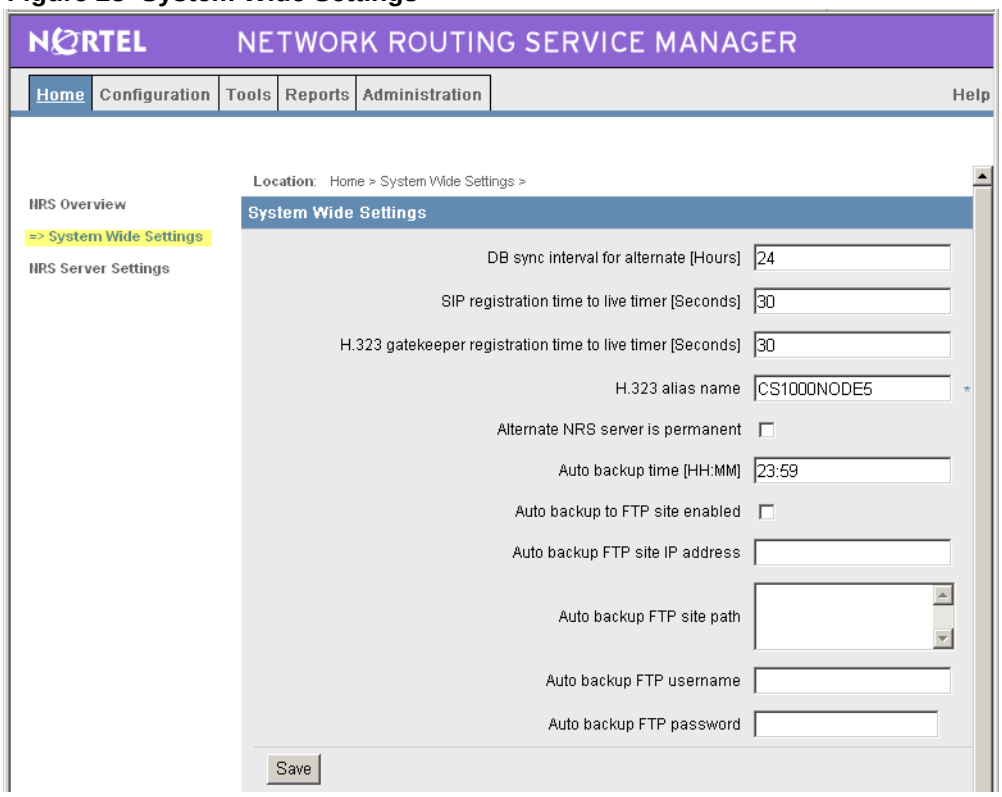
End

Verifying and adjusting system-wide settings

You can check system-wide settings and make changes from NRS Manager.

Step	Action
1	Log on to NRS Manager.
2	Select **System Wide Settings**. The System Wide Settings page appears. See Figure 28 "System Wide Settings" (page 63).

Figure 28 System Wide Settings



3 Configure the information in the System Wide Settings page.

Refer to Table 4 "System Wide Settings — fields description" .

Table 4 System Wide Settings — fields description (Sheet 1 of 2)

Field	Description
DB Synch interval for alternate [Hours]	24 is the default.
SIP registration Time-to-Live timer	30 seconds is recommended.
H.323 Gatekeeper registration Time-to-Live timer	30 seconds is recommended.
H.323 Alias Name	This is a mandatory field. The H.323 Alias Name must be alphanumeric and contain no spaces. The default value is the same as the H.323 ID and HostName value configured in the PRIMARY Signaling Server's *config.ini* file.
Alternate NRS server is permanent	Select this check box if the Alternate NRS Server is to remain in service after a switch-over, even if the Primary NRS recovers. Clear the check box if the Alternate NRS switches over functions to the Primary NRS Server after the Primary NRS Server recovers.

Table 4 System Wide Settings — fields description (Sheet 2 of 2)

Field	Description
Auto backup time	Enter the time when the database backup automatically occurs.
Auto backup to FTP site enabled	Select this check box to enable automatic backup of the NRS database to an FTP site.
Auto backup FTP site IP address **Auto backup FTP site path** **Auto backup FTP site username** **Auto backup FTP site password**	Enter values for Autobackup FTP if you enabled automatic backup of the NRS database to an FTP site.

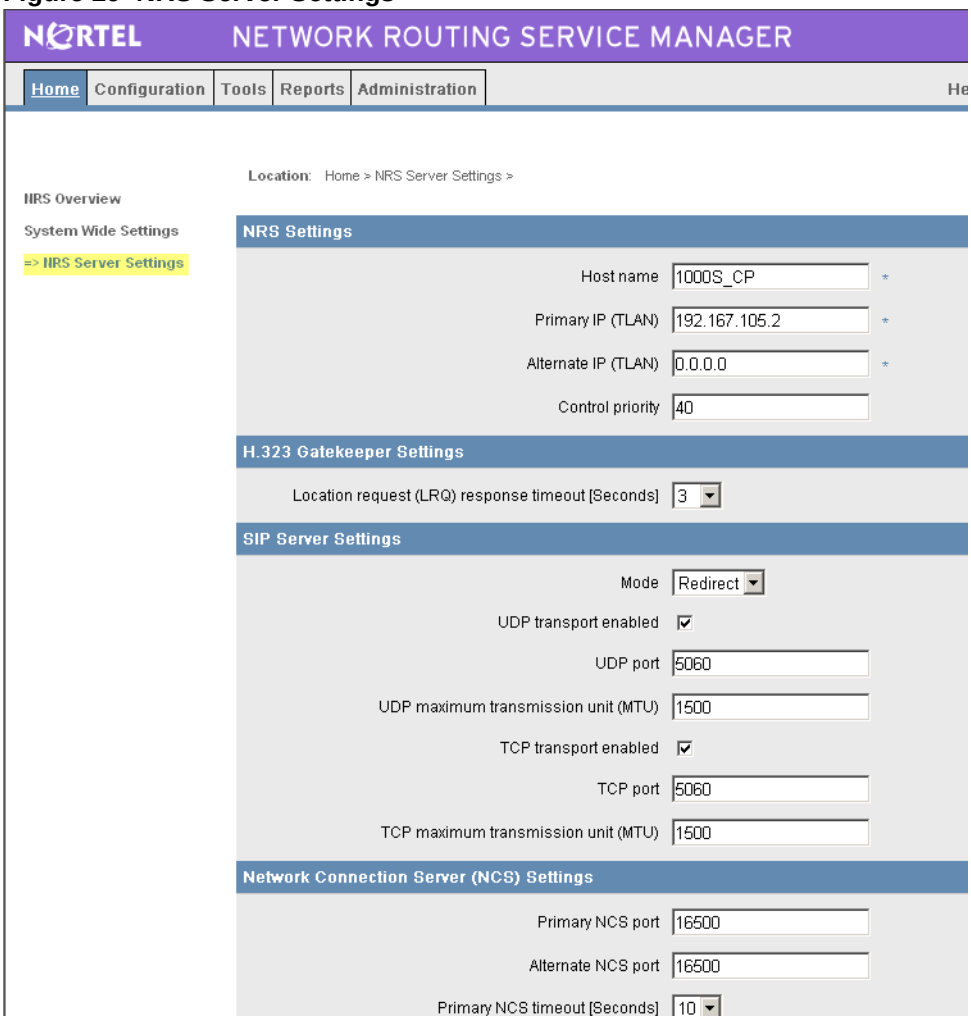
4 Click **Save**.

End

Configuring the NRS server settings (H.323 Gatekeeper or SIP)

Step	Action
1	Log on to NRS Manager.
2	Select **NRS Server Settings**. The NRS Server Settings page appears. See Figure 29 "NRS Server Settings" (page 65).

Figure 29 NRS Server Settings



3 Under **NRS Settings**, set the following values:

- Host name
- Primary IP (T-LAN)
- Alternate IP (T-LAN)
- Control priority

4 Under **H.323 Gatekeeper Settings**, select the **Location request (LRQ) response timeout**.

5 Under **SIP Server Settings**, set the following values:

- Mode
- UDP transport enabled/disabled
- UDP port
- UDP maximum transmission unit (MTU)
- TCP transport enabled/disabled
- TCP port

- TCP maximum transmission unit (MTU)

Note: Make the values under **SIP Server Settings** the same as those you configure for the SIP Proxy in Element Manager.

6 Under **Network Connection Server (NCS) Settings**, set the following values:

- Primary NCS IP address and port number
- Alternate NCS IP address and port number
- Primary NCS timeout

7 Click **Save**.

End

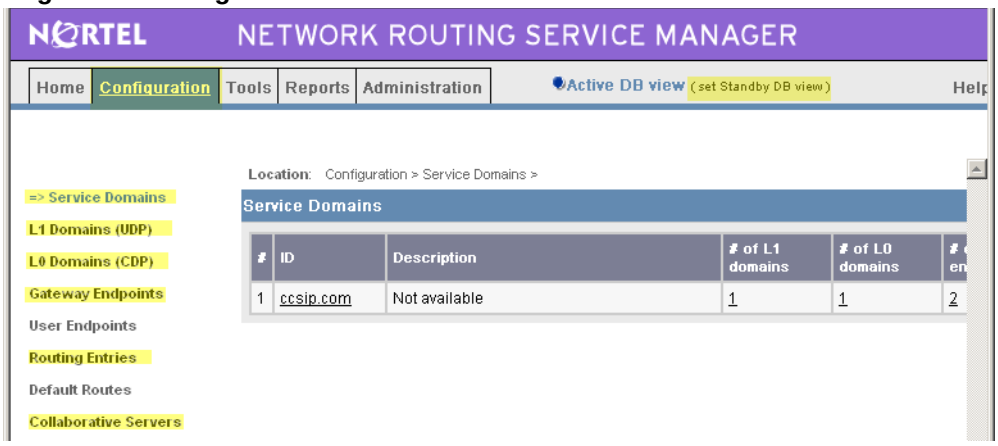
Configuring the service domain

The NRS database information configured in this procedure is required by both the SIP Redirect Server and the H.323 Gatekeeper.

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab.
3	Click **Standby DB View** to switch from active to standby database view. See Figure 30 "Configuration".

Note: The active database view is the default view. Use the active database for runtime queries, and the standby database for administrator modifications. You must use standby view to make changes to the database.

Figure 30 Configuration

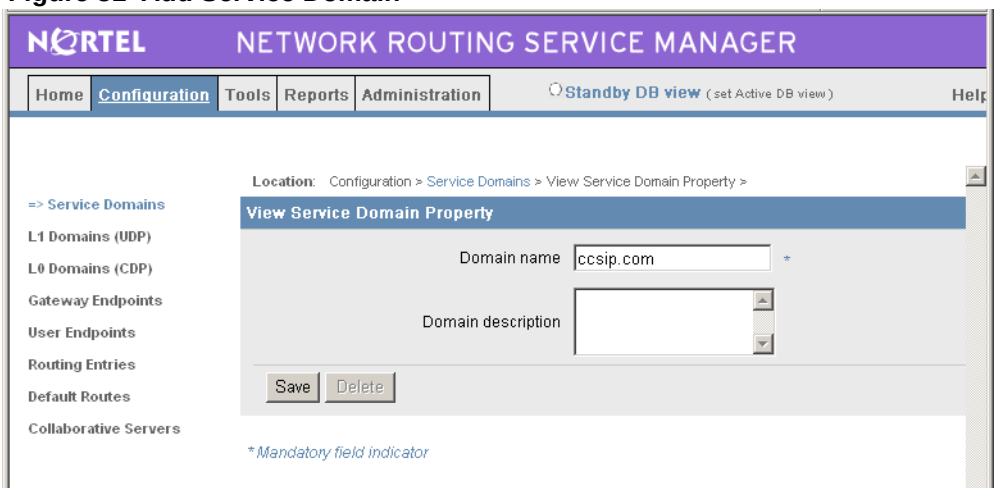


4 Select **Service Domains**.

5 Click **Add**.

The Add Service Domain Property page appears. See Figure 31 "Add Service Domain".

Figure 31 Add Service Domain



6 Enter your **Domain name** and a **Domain description**.

These values must match that set for the Signaling Server.

7 Click **Save**.

The Service Domains page appears again with the new domain added.

Note: When no description is entered, the service domain is shown with the message “Not available”. This means that the description is not entered, but the service domain is still active. This applies to all description fields in NRS Manager.

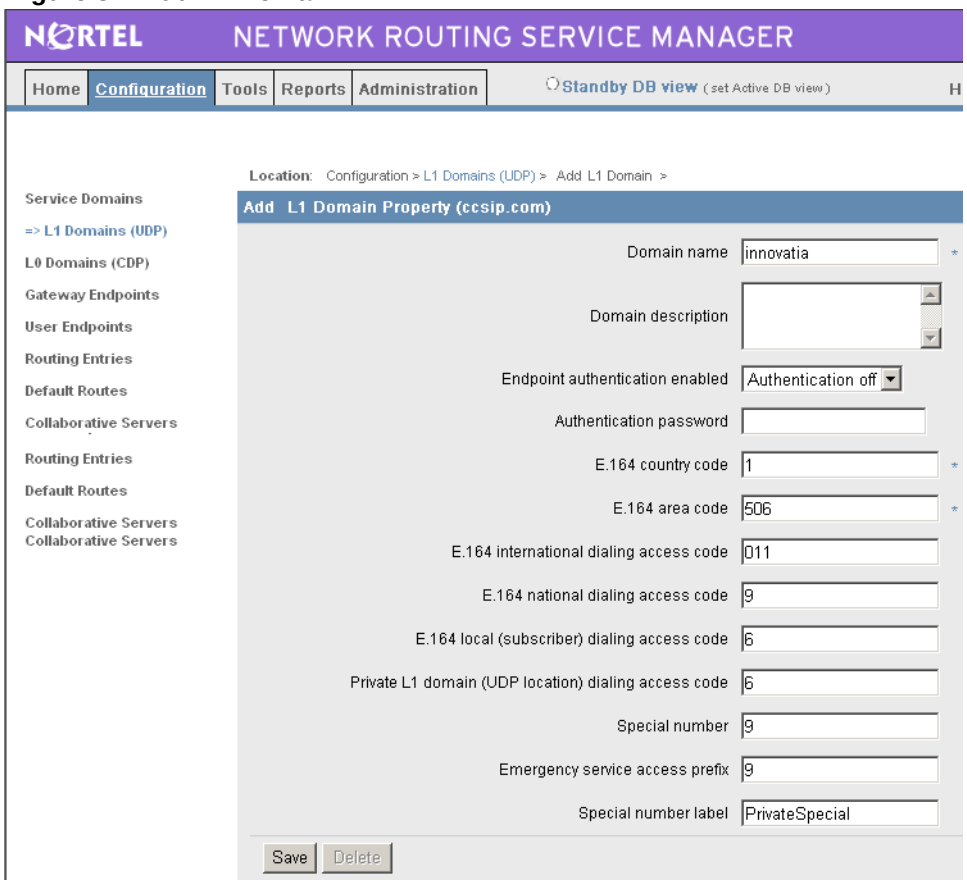
End

Configuring the L1 domain (UDP)

You can configure the L1 domain after you configure the service domain. The L1 domain is a service domain associated with UDP.

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab.
3	Click **Standby DB View** to switch from active to standby database view. See Figure 30 "Configuration" (page 66).
4	Select **L1 Domains**.
5	Click **Add**. The Add L1 Domain page appears. See Figure 32 "Add L1 Domain" (page 68).

Figure 32 Add L1 Domain



6 Configure the L1 domain.

Refer to Table 5 "L1 domain fields" for configuration information.

Table 5 L1 domain fields (Sheet 1 of 2)

Field	Value	Description
Domain name	<alphanumeric string>	Mandatory. The name must be alphanumeric and can be up to 30 characters in length.
Domain description	<character string>	Optional. The description can include any character except single quotes and be up to 120 characters in length.
Endpoint authentication enabled	Authentication off Authentication on	If Authentication on is selected, all endpoints require authentication.
Authentication password	<alphanumeric string>	If Authentication on is selected, enter an authentication password. The password must be alphanumeric and up to 30 characters in length.
E.164 country code	<numeric string>	Mandatory. The code must be numeric and up to 7 characters in length.
E.164 area code	<numeric string>	Mandatory. The code must be numeric and up to 7 characters in length.

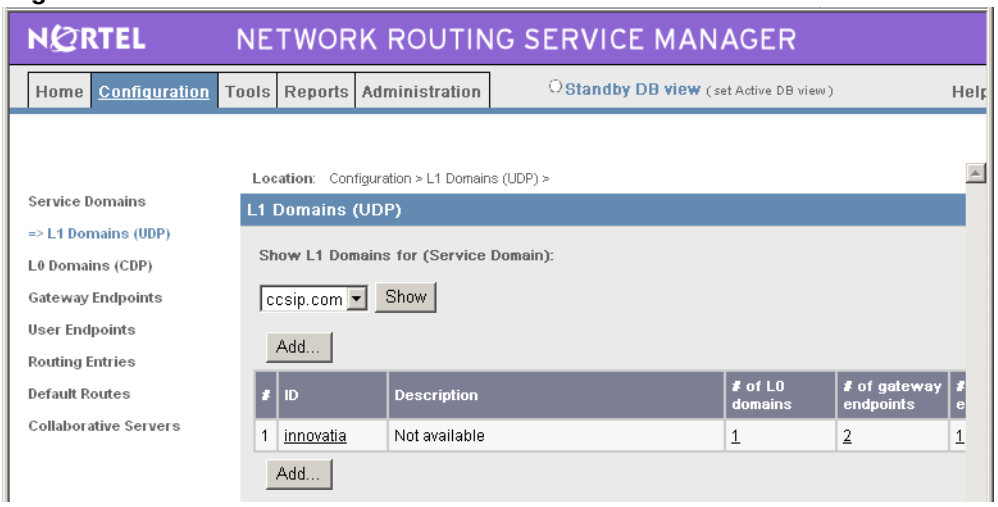
Table 5 L1 domain fields (Sheet 2 of 2)

Field	Value	Description
E.164 International Dialing Access Code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 national dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 local (subscriber) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Private L1 domain (UDP) location) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Special number	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.
Emergency service access prefix	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.
Special number label	<alphanumeric string	Optional. The label must be alphanumeric and up to 30 characters in length. The first character in the label must be alphabetic.

7 Click **Save**.

The L1 Domains page appears again with the new L1 domain added. See Figure 33 "L1 Domains".

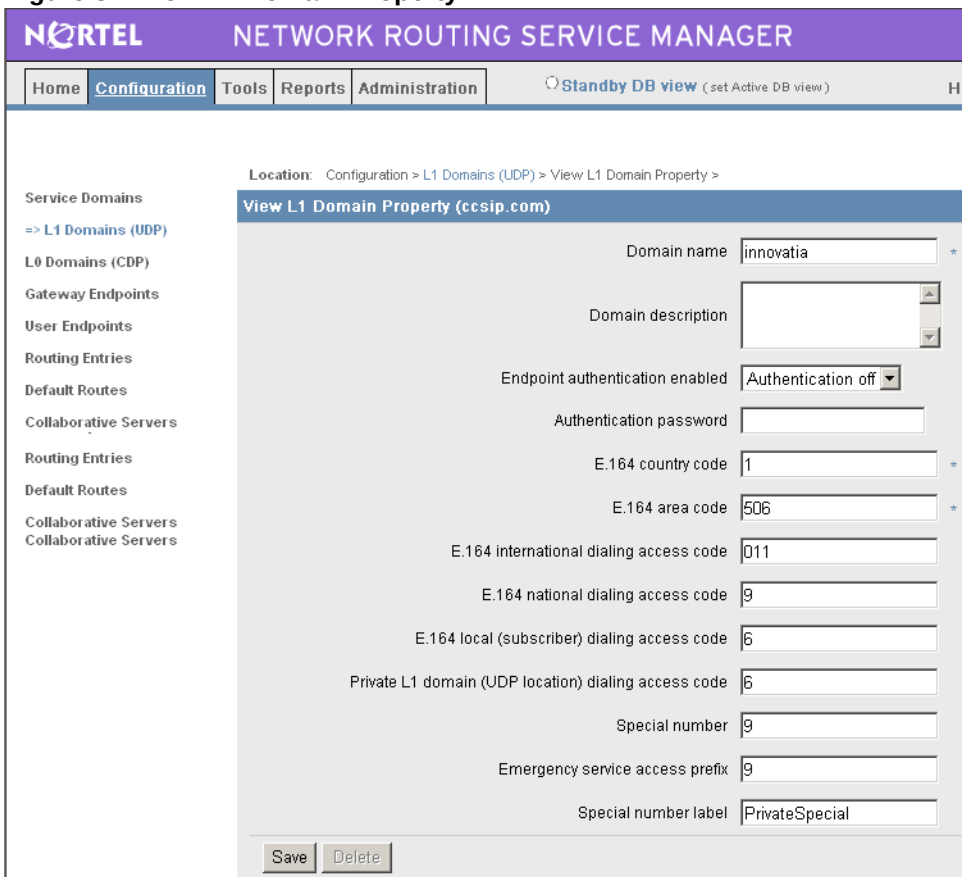
Figure 33 L1 Domains



8 To view the configured data for the L1 domain, click the **ID** in the **L1 Domains (UDP)** menu.

The View L1 Domain Property page appears, displaying your configured data. See Figure 34 "View L1 Domain Property".

Figure 34 View L1 Domain Property



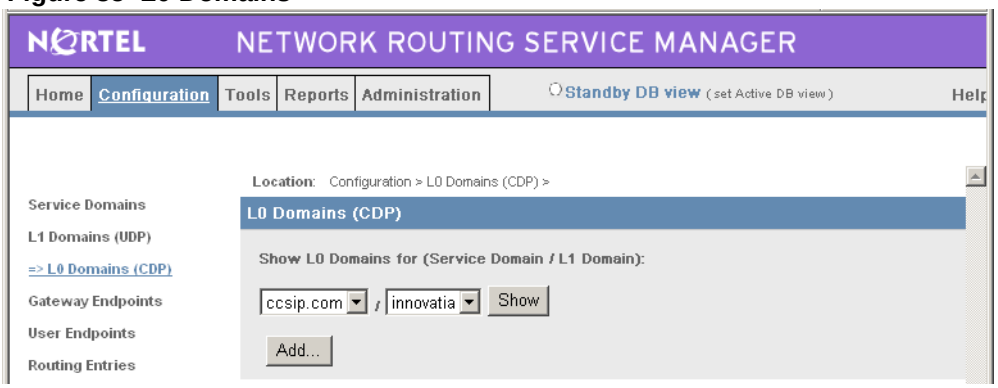
End

Configuring the L0 domain (CDP)

The L0 domain is a service domain associated with CDP, representing the private addresses field in the SIP URI. This address is composed of the service, L1, and L0 domains.

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab.
3	Click **Standby DB View** to switch from active to standby database view. See Figure 30 "Configuration" (page 66).
4	Click **L0 Domains**. The L0 Domains page appears. See Figure 35 "L0 Domains" (page 71).

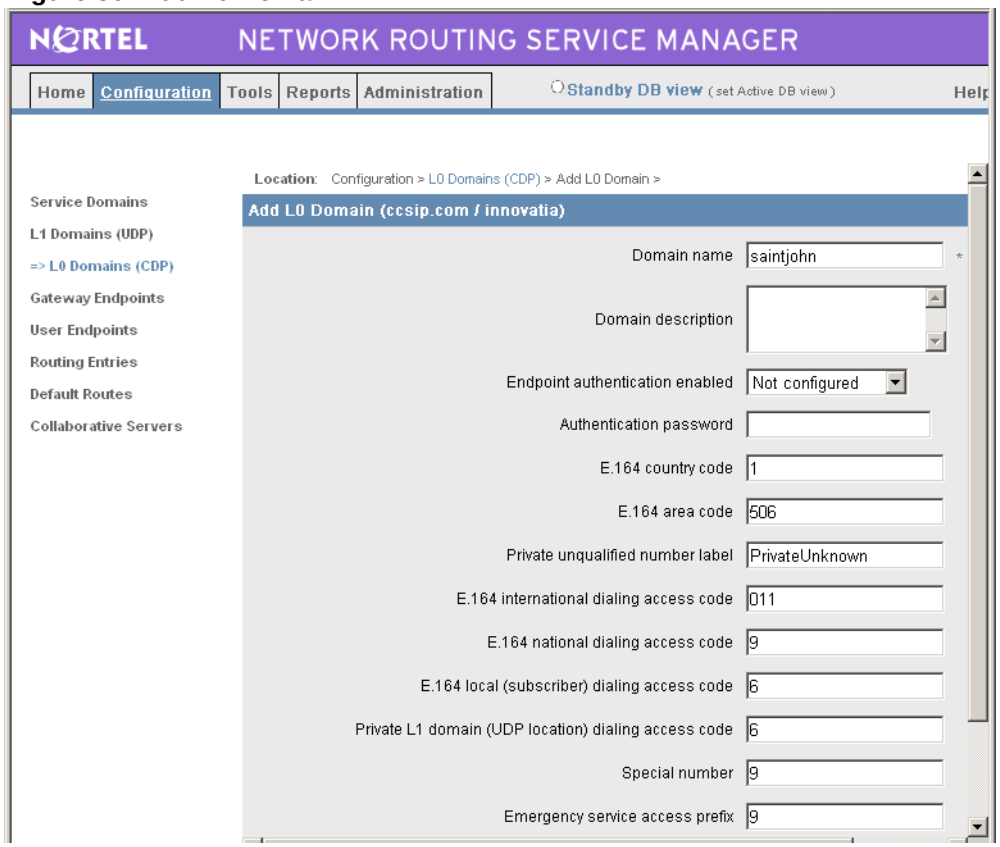
Figure 35 L0 Domains



5 Click **Add**.

The Add L0 Domain window appears. See Figure 36 "Add L0 Domain".

Figure 36 Add L0 Domain



6 Enter the appropriate values for your network.

Refer to Table 6 "Add L0 Domain fields" (page 72) for configuration information.

Note: The country codes, area codes, public prefixes, and private prefixes must match those of your L1 domain.

Table 6 Add L0 Domain fields

Field	Value	Description
Domain name	<alphanumeric string>	Mandatory. The name must be alphanumeric and can be up to 30 characters in length.
Domain description	<character string>	Optional. The description can include any character except single quotes and can be up to 120 characters in length.
Endpoint authentication enabled	Authentication off Authentication on	If Authentication on is selected, then all endpoints require authentication.
Authentication password	<alphanumeric string>	if Authentication on is selected, enter a password. The password must be alphanumeric and up to 30 characters in length.
E.164 country code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 area code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Private unqualified number label	<alphanumeric string>	The label must be alphanumeric and up to 30 characters in length. The first character in the label must be alphabetic.
E.164 international dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 national dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 local (subscriber) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Private L1 domain (UDP) location) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Special number	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.
Emergency service access prefix	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.

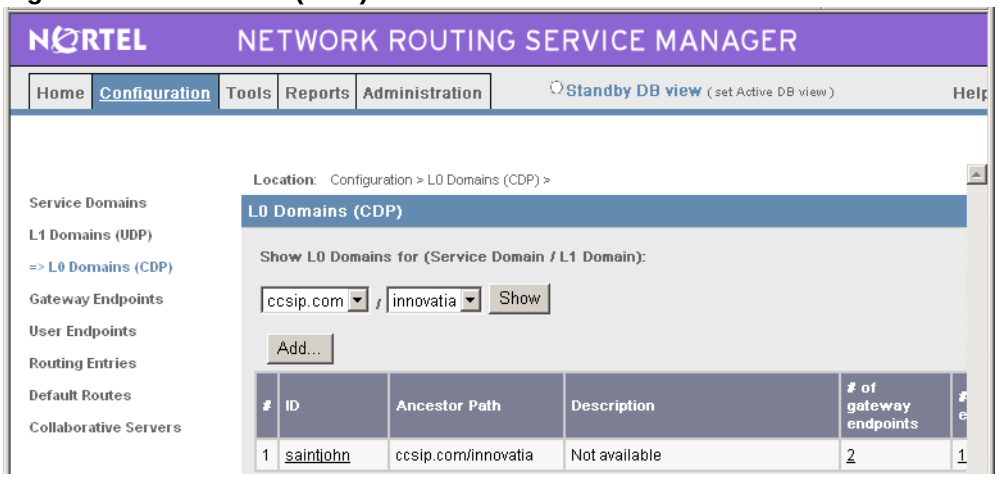
7 Click **Save**.

The L0 Domains page appears again, showing the added domain.

8 To view the configured data, select the service domain and L1 domain and click **Show**.

A list of configured L0 domains appears. See Figure 37 "L0 Domains (CDP)".

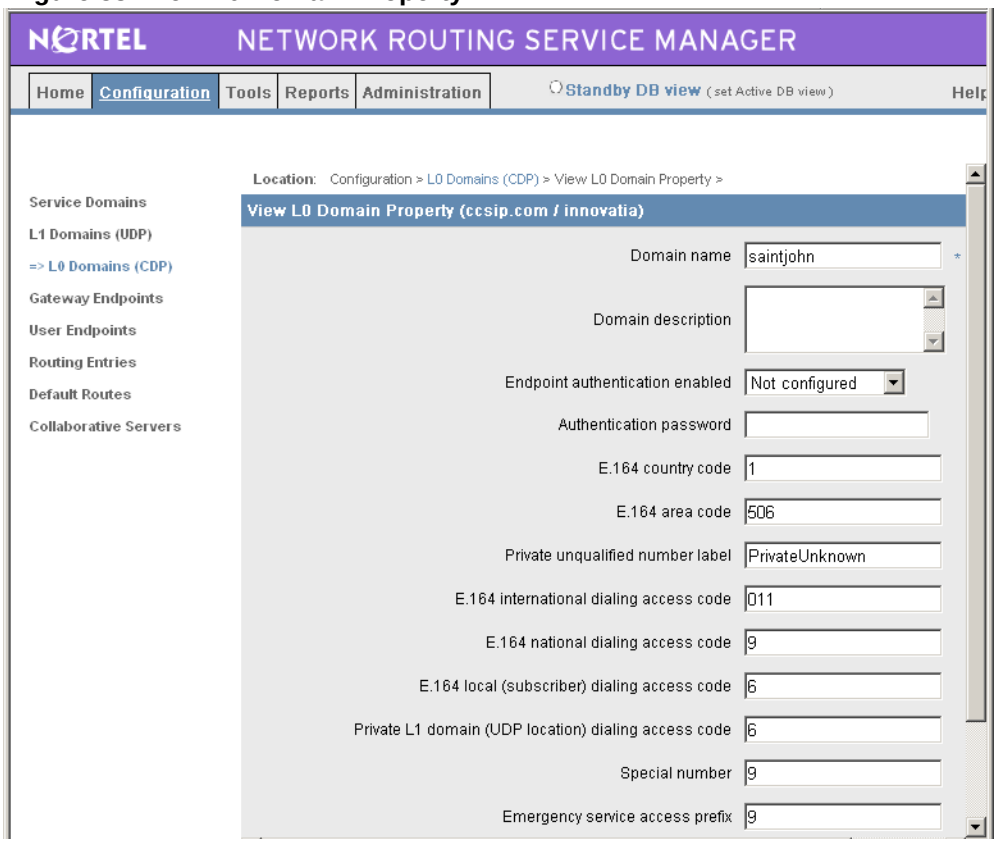
Figure 37 L0 Domains (CDP)



9 Select the L0 domain for which you would like to see configuration information.

The View L0 Domain Property page appears. See Figure 38 "View L0 Domain Property".

Figure 38 View L0 Domain Property



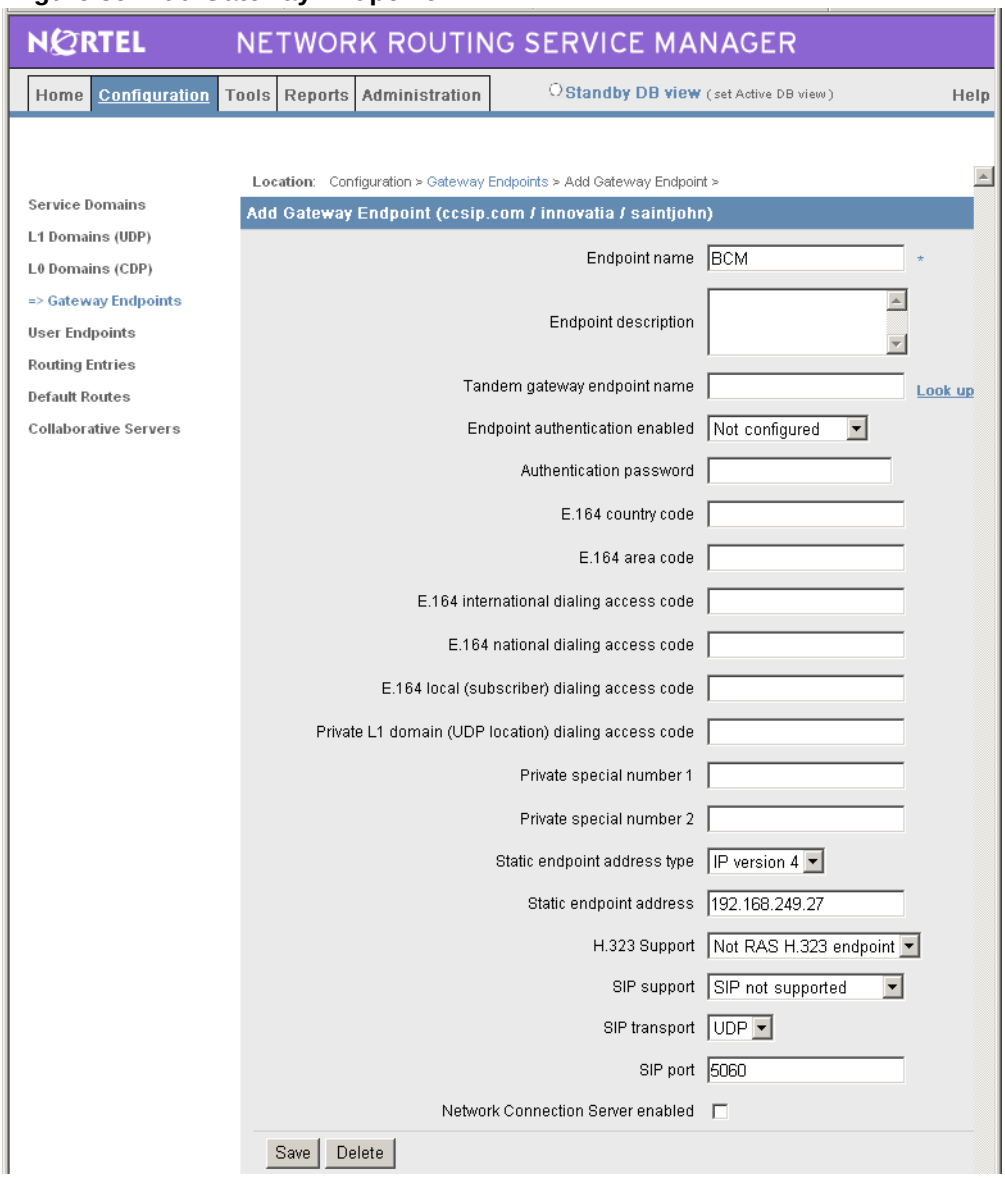
End

Configuring Gateway endpoints

Add an endpoint for both the Communication Server 1000 and Business Communications Manager (BCM).

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab
3	Click **Standby DB View** to switch from active to standby database view.
4	Click **Gateway Endpoints**. See Figure 30 "Configuration" (page 66).
5	Click **Add**. The Add Gateway Endpoint page appears. See Figure 39 "Add Gateway Endpoint".

Figure 39 Add Gateway Endpoint



6 Enter the appropriate values for your network.

Refer to Table 7 "Add Gateway Endpoint fields" for configuration information.

Tip: This is a Gateway endpoint, which can be served by several users. You can add multiple endpoints, some SIP-only, some H.323-only, and Unistim. You can also configure a user endpoint, which can be only one of these three protocols.

Table 7 Add Gateway Endpoint fields (Sheet 1 of 3)

Field	Value	Description
Endpoint name	<alphanumeric string>	The name must be alphanumeric and up to 30 characters in length.
Endpoint Description	<alphanumeric string>	The description must be alphanumeric and up to 120 characters in length.
Tandem Gateway endpoint name	<alphanumeric string>	The tandem Gateway is optional. This indicates whether the endpoint is used to tandem calls from outside the network. The name must be alphanumeric and up to 30 characters in length. **Note**: Use the Look-up link to find configured Gateway endpoints.
Endpoint authentication enabled	Not configured	If this option is selected, the Gateway endpoint uses the L1 or L0 authentication (if enabled).
	Authentication off	If this option is selected, authentication is off for this Gateway endpoint even if L1 or L0 authentication is enabled.
	Authentication on	If this option is selected, authentication is on for this Gateway endpoint, and the authentication overrides the L1 or L0 authentication (if enabled).
Authentication password	<alphanumeric string>	If Authentication on is selected, choose a password. The password must be alphanumeric and up to 30 characters in length.
E.164 country code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 area code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 international dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 national dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.

Table 7 Add Gateway Endpoint fields (Sheet 2 of 3)

Field	Value	Description
E.164 local (subscriber) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Private L1 domain (UDP) location) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Private special number 1	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.
Private special number 2	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.
Static endpoint address type	IP version 4	Select IP version 4 from the drop-down list.
Static endpoint address	<Node IP address>	This is the Node IP address of the Signaling Server. If a third-party Gateway is used, it is the IP address of the Gateway.
H.323 support	H.323 not supported RAS H.323 endpoint Not RAS H.323 endpoint	RAS H.323 Endpoint is recommended. If an H.323 Gateway Endpoint is configured with an H.323 Support type of RAS H.323 endpoint, NRS Manager displays Endpoint Dynamic Registration information after the H.323 Gateway registers with the NRS. Endpoint Dynamic Registration information includes Call Signaling IP, RAS IP, Alias name, t35Country code, t35Extension, Manufacturer code, Product ID, and Version ID.
SIP support	SIP not supported Static SIP endpoint Dynamic SIP endpoint	Dynamic SIP Endpoint is recommended. If a SIP Trunk Gateway Endpoint is configured with a SIP Support type of Dynamic SIP endpoint, NRS Manager displays Endpoint Dynamic Registration Information for SIP after the SIP Trunk Gateway registers with the NRS. Endpoint Dynamic Registration Information includes SIP IP, Registration expiry time, User agent, and Preference.
SIP transport	TCP UDP	TCP is selected by default. This information should match the SIP Transport Protocol in the Signaling Server Properties.
SIP port	<port value>	Default SIP port value is 5060. If the SIP Port is changed, the value must be numeric and up to 5 numbers in length. The range is 0 to 65535.

Table 7 Add Gateway Endpoint fields (Sheet 3 of 3)

Field	Value	Description
Network Connection Server enabled	<check box>	Select the Network Connection Server is enabled check box if this Gateway Endpoint supports the NCS for branch office or SRG user redirection to the main office, Virtual Office, or Geographic Redundancy.

7 Click **Save**.

The Gateway Endpoints window appears again with the new endpoints added.

8 From the Gateway Endpoint page, select the **Service**, **Domain**, **L1 domain**, and **L0 domain** to view the configured data of an endpoint.

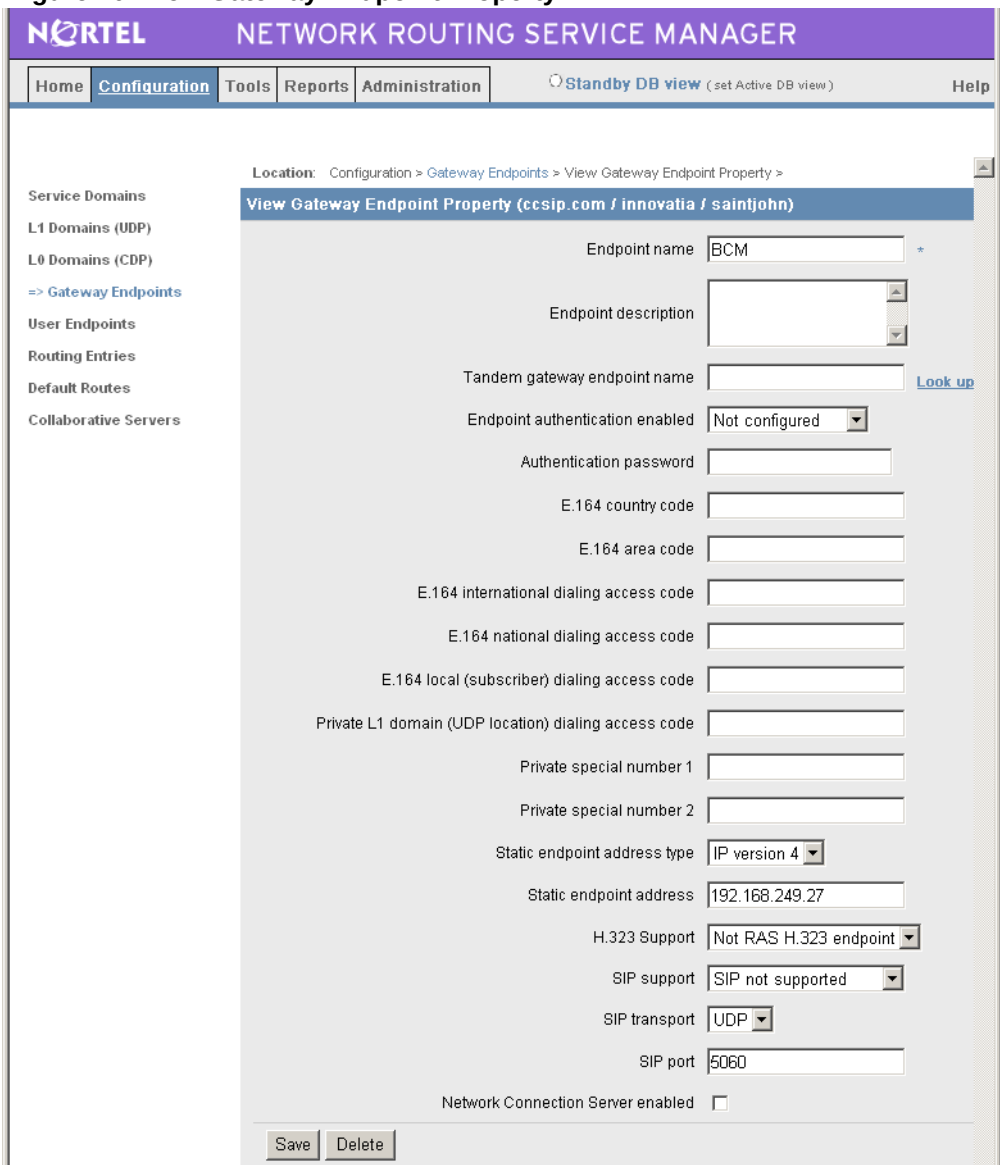
9 Click **Show**.

A list of configured Gateways appears.

10 Click the **Gateway ID** you wish to view.

The **View Gateway Endpoint Property** page appears. See Figure 40 "View Gateway Endpoint Property" (page 78).

Figure 40 View Gateway Endpoint Property



End

Configuring routing entries

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab.
3	Click **Standby DB View** to switch from active to standby database view.
4	Click **Routing Entries**.
5	Type the relevant **Gateway endpoint**. Click the **Look up** link and perform a search. All configured endpoints appear.

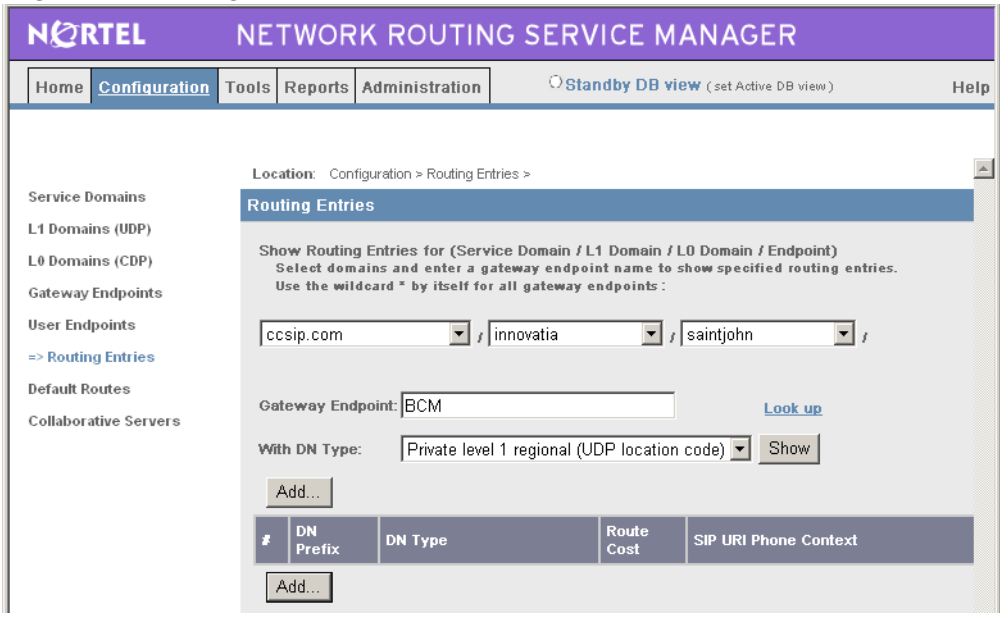
6 Click the endpoint to configure as a Routing Entry.

7 Select a **DN** type. For **UDP**, select **Private level 1 regional**.

8 Click **Show**.

The Routing Entries page appears. See Figure 41 "Routing Entries".

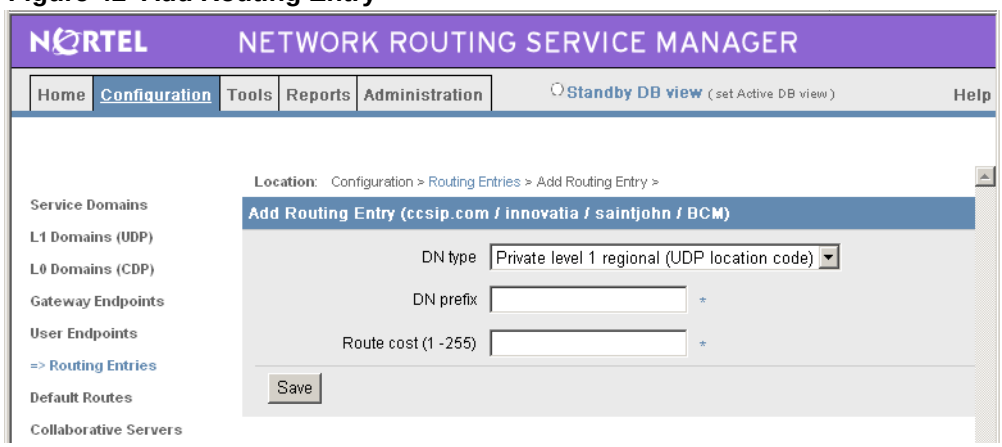
Figure 41 Routing Entries



9 Click **Add** for the Routing Entry.

The Add Routing Entry page appears. See Figure 42 "Add Routing Entry".

Figure 42 Add Routing Entry



10 Enter the **DN prefix** if the **Default route** is blank.

This is the CDP DSC steering code.

11 Enter the **Route cost**.

The higher the number, the higher the cost. This is equivalent to Least Cost Routing.

12 Click **Save**.

End

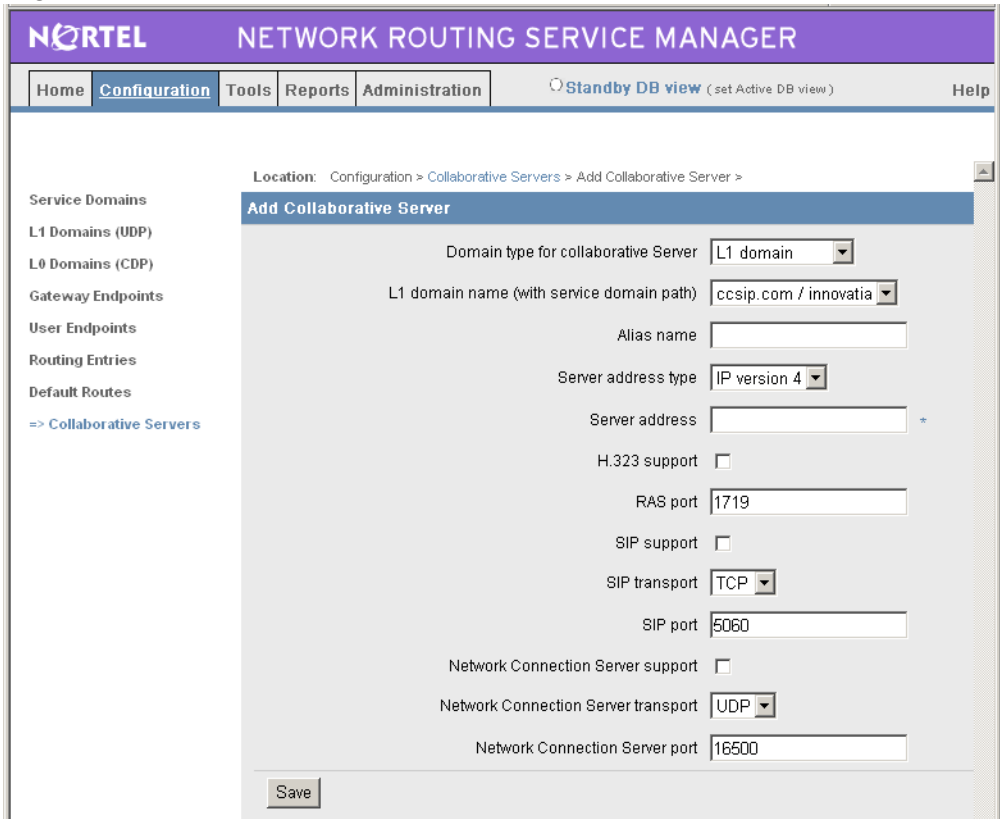
Configuring collaborative servers

A Collaborative Server is a server in another network zone that can resolve requests when your NRS cannot find a match in its numbering plan database.

You can specify a list of Networking Routing Servers in different network zones in your NRS. The NRS Manager provides a utility for adding and viewing a list of NRSs (Collaborative Servers) in different network zones.

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab.
3	Click **Standby DB View** to switch from active to standby database view.
4	Click **Collaborative Servers**. The Collaborative Servers page appears. See Figure 30 "Configuration" (page 66).
5	Click **Add**. The Add Collaborative Server page appears. See Figure 43 "Add Collaborative Server". This page may differ from the view shown here depending on the value you choose for the **Domain type for collaborative server**.

Figure 43 Add Collaborative Server



6	For **Domain type for collaborative Server**, select either **L0 domain** or **L1 domain**.
7	For the **L1** or **L0 domain name**, select the L1 or L0 Domain name.

8 Enter the **Alias name** of the Collaborative Server. The alias name must be alphanumeric and contain no spaces.

9 From the **Server address type** menu, select **IP version 4**.

10 For **Server address**, type the server IP address.

11 If the H.323 protocol is supported by the server, populate the following fields:

- **H.323 support** check box
- **RAS port**

12 If the SIP protocol is supported by the server, populate the following fields:

- **SIP support** check box
- **SIP transport** protocol
- **SIP port**

13 If Network Connection Service is supported by the server, populate the following fields:

- **Network Connection Server support** check box
- **Network Connection Server transport**
- **Network Connection Server port**

14 Click **Save**.

The Collaborative Servers page appears with the new server.

15 For redundancy purposes, perform this procedure again for the alternate NRS in the other network zone.

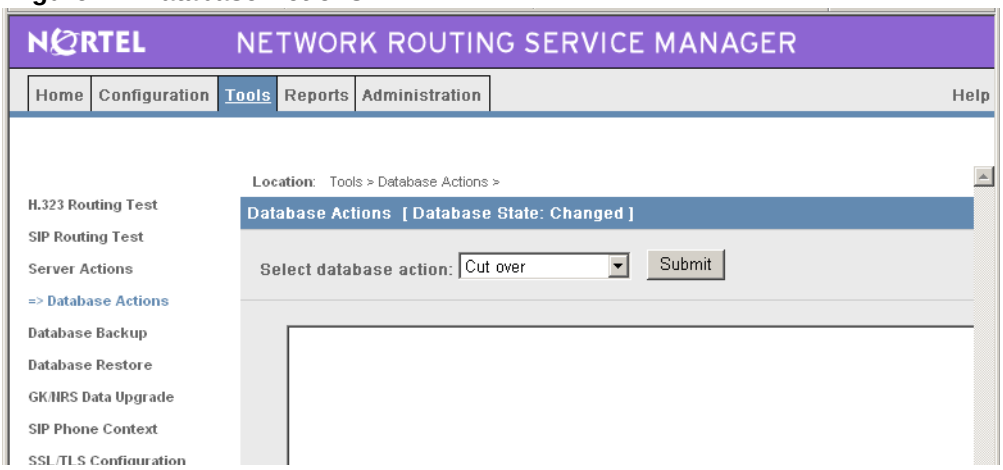
End

Updating the database

To save your entries, you must update the database.

Step	Action
1	Log on to NRS Manager.
2	Click the **Tools** tab.
3	Click the **Database Actions** tab. The Database Actions page appears, showing the **Database State** as **Changed**. See Figure 44 "Database Actions" (page 82).

Figure 44 Database Actions

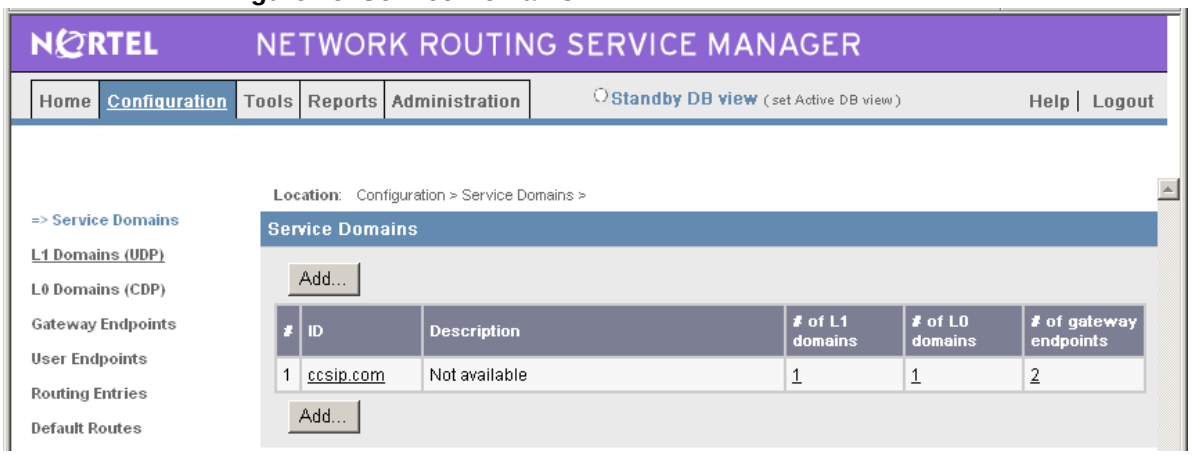


End

Checking the status of registered endpoints

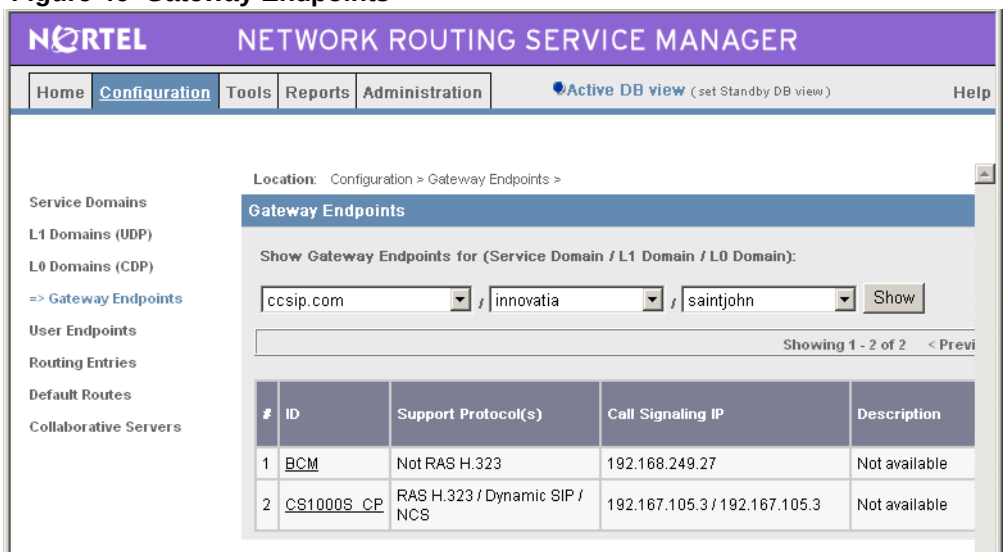
Step	Action
1	Log on to NRS Manager.
2	Click the **Configuration** tab.
3	Select **Service Domains**. See Figure 45 "Service Domains".

Figure 45 Service Domains



4	Click **Active DB View** to switch from standby to active database view.
5	Click the number in the **# of Gateway endpoints** column. The Gateway Endpoints page appears. See Figure 46 "Gateway Endpoints" (page 83).

Figure 46 Gateway Endpoints



6 Click **Show**.

All endpoints appear as “Connected”. You can see that the endpoints are configured for both the H.323 and SIP protocols.

End

Performing an H.323 routing test

Step	Action

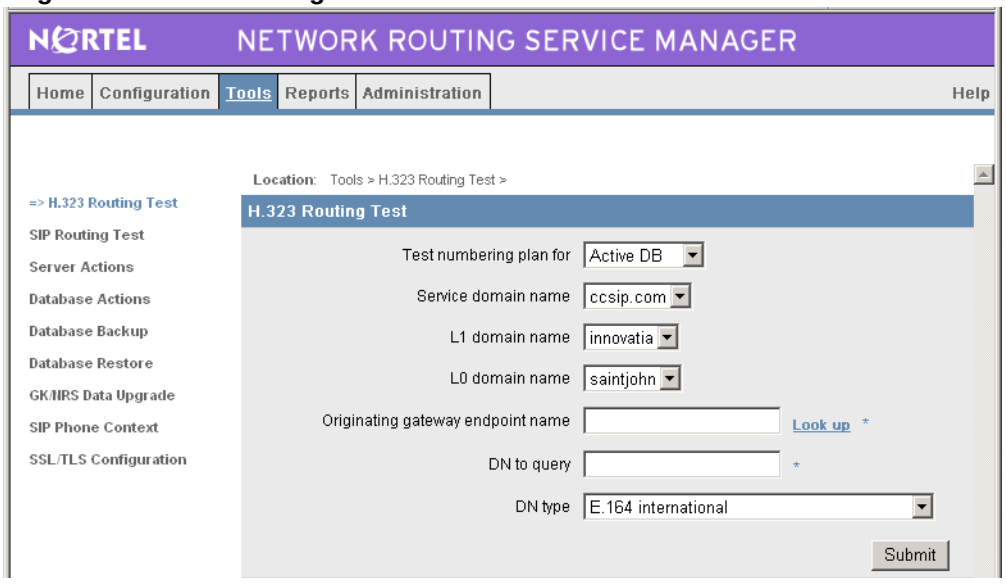
1 Log on to NRS Manager.

2 Click the **Tools** tab.

3 Select **H.323 Routing Test**.

See Figure 47 "H.323 Routing Test".

Figure 47 H.323 Routing Test



4 For **Test numbering plan for**, select **Active DB**.

5 Select your domain names if they are not autopopulated.

6 **Look up** and select the **Originating gateway endpoint name**.

7 Type a **DN to query**.

8 Select the **DN type**.

9 Click **Submit**.

End

Checking the status of virtual D-channels

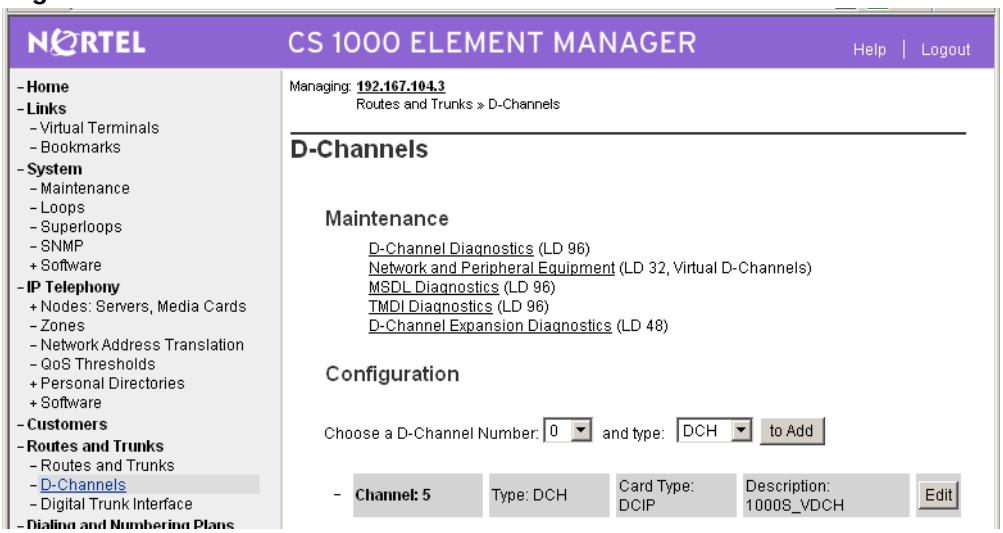
Step	Action

1 Log on to Element Manager.

2 Select **Routes and Trunks > D-Channels**.

The D-Channels page appears. See Figure 48 "D-Channels".

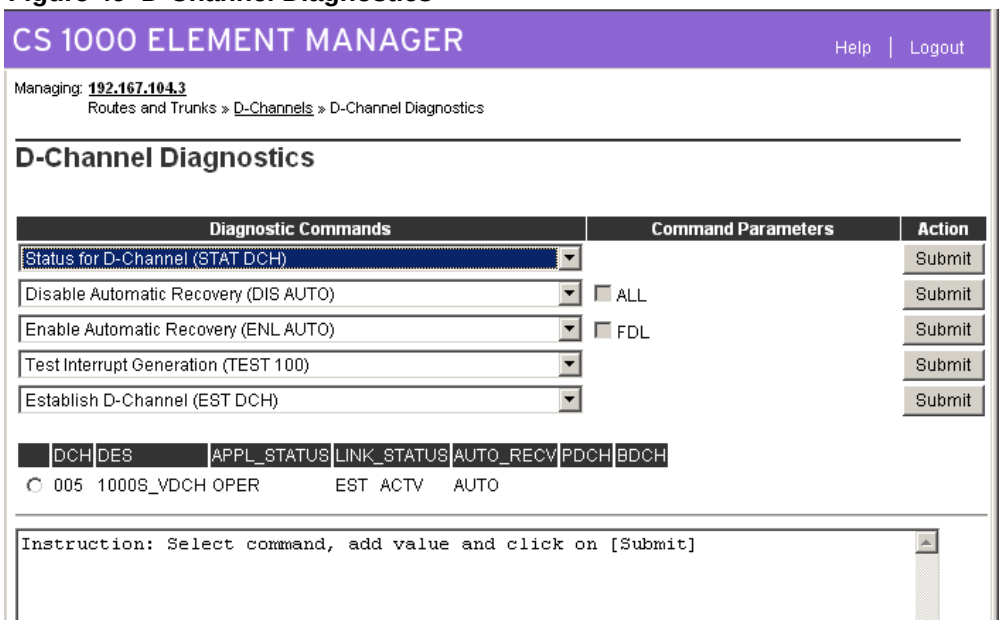
Figure 48 D-Channels



3 Select **D-Channel Diagnostics (LD 96)**.

The D-Channel Diagnostics page appears. See Figure 49 "D-Channel Diagnostics" (page 85).

Figure 49 D-Channel Diagnostics



4 Under **Diagnostic Commands**, select **Status for D-Channel (STAT DCH)**.

5 Click **Submit**.

6 Check that the D-Channel is operational, established, and active.

End

Checking the status of virtual trunks

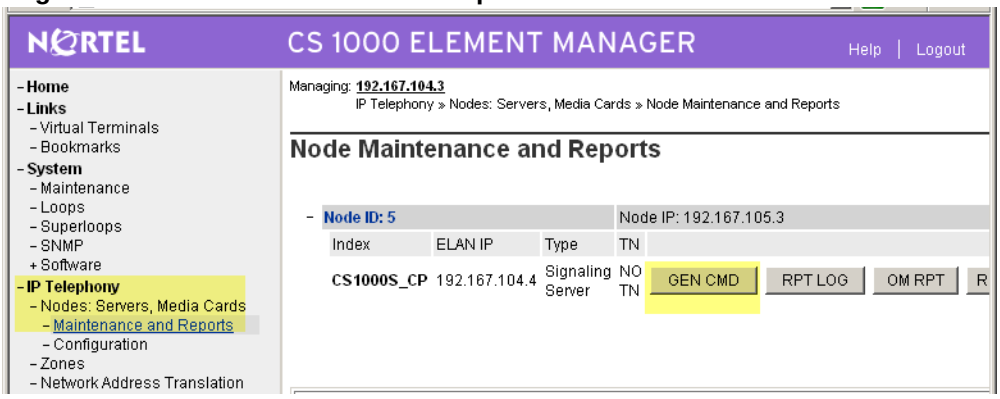
Step	Action

1 Log on to Element Manager.

2 Select **IP Telephony > Nodes: Servers, Media Cards > Maintenance and Reports**.

See Figure 50 "Node Maintenance and Reports".

Figure 50 Node Maintenance and Reports

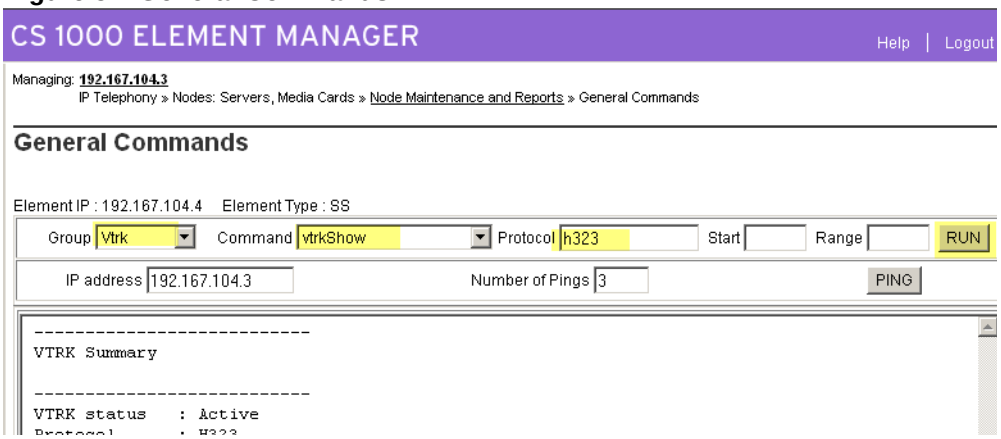


3 Expand the **Node ID** heading.

4 Click **GEN CMD** for the switch.

The General Commands page appears. See Figure 51 "General Commands".

Figure 51 General Commands



5 For **Group**, select **Vtrk**.

6 For **Command**, select **vtrkShow**.

7 For **Protocol**, type **H323**.

8 Click **Run**.

The Virtual Trunk status appears.

9 Check each IP Phone manually.

At the **DEF GW** option, verify that the IP address is the same as the T-LAN Gateway of that system.

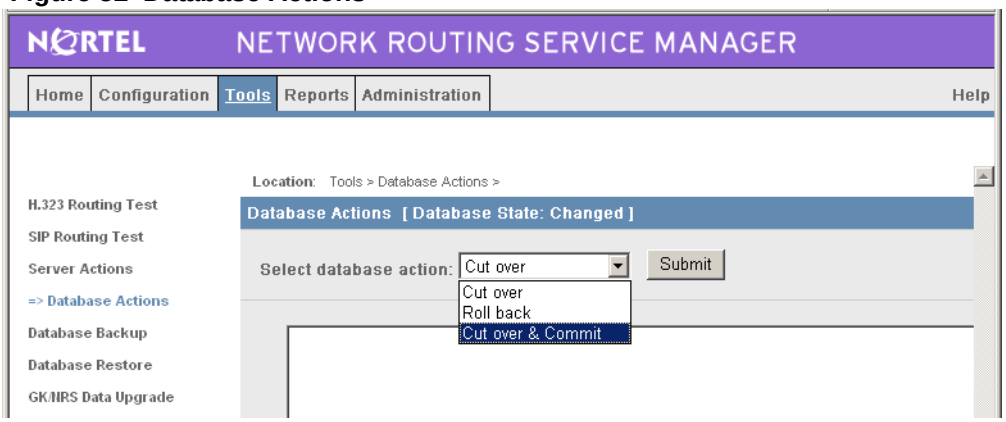
Tip: If the phones ring and have dial tone but there is no speech path, the Default Gateway is 0.0.0.0 and is not operational.

Committing Gatekeeper configuration changes

Gatekeeper changes occur in the standby database. If you want the active Gatekeeper to use these settings, you must commit them to the active database from the Gatekeeper Admin tool.

Step	Action
1	Log on to NRS Manager.
2	Click the **Tools** tab.
3	From the left navigation pane, select **Database Actions**. See Figure 52 "Database Actions" (page 87).

Figure 52 Database Actions



4 Select **Cut over & Commit**.

5 Click **Submit**.

End

BCM 200/400 configuration

This chapter describes configuration procedures for the Business Communications Manager (BCM) 200 and 400 systems.

Note: Element Manager as viewed on your system may differ slightly from the screens shown in this chapter because you can customize the column display in Element Manager.

BCM 200/400 configuration procedures

The sequence of BCM 200/400 configuration procedures is as follows:

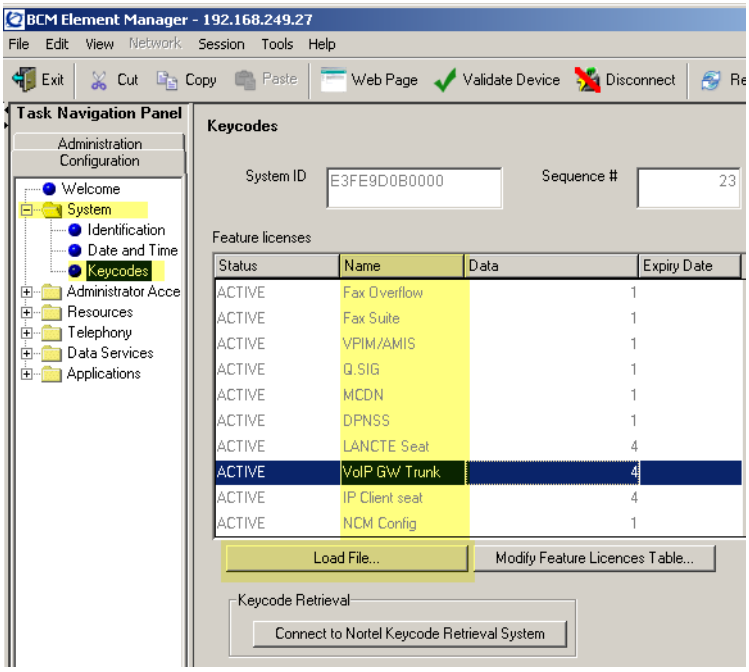
- "Configuring incoming VoIP trunks" (page 89)
- "Verifying system license and keycodes" (page 90)
- "Configuring VoIP trunk media parameters" (page 90)
- "Configuring local Gateway parameters" (page 94)
- "Configuring VoIP lines" (page 99)
- "Configuring target lines" (page 103)

Configuring incoming VoIP trunks

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **System** > **Keycodes**. See Figure 53 "Keycodes" (page 90).
4	Load new Keycodes by loading a new keycode file or connecting to Nortel's Keycode Retrieval System (KRS).

Note: For more information about keycodes and keycode retrieval, see *Keycode Installation Guide* (NN40010-301).

Figure 53 Keycodes



End

Verifying system license and keycodes

Determine the IP Trunk count.

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **System** > **Keycodes**. See Figure 53 "Keycodes".
4	In the **Name** column, scroll down to **VoIP GW Trunk**. The number of license keys you have are listed in the Data column.

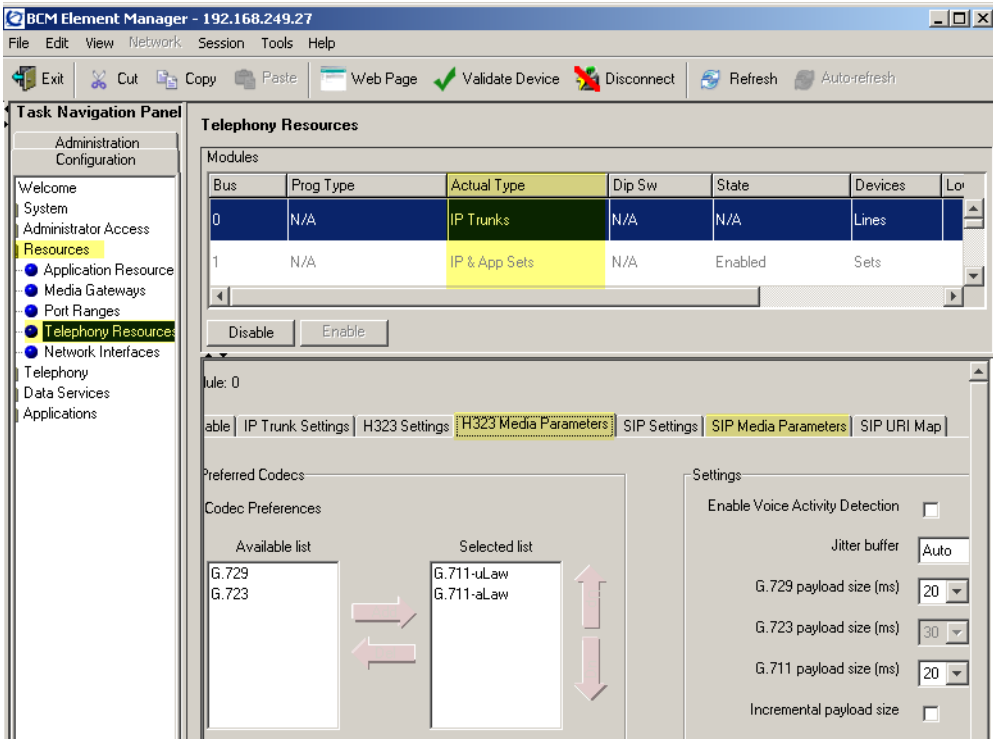
End

Configuring VoIP trunk media parameters

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **Resources > Telephony Resources**. See Figure 54 "Telephony Resources" (page 91).

4 In the **Modules** panel, select the line where the **Actual Type** column is set to **IP Trunks**.

Figure 54 Telephony Resources



5 Select the **H.323 Media Parameters** or **SIP Media Parameters** tab.

6 Enter the information that supports your system.

Ensure that these settings are consistent with the other systems on your network.

Refer to the tables Table 8 "H.323 Media Parameters — fields description" and Table 9 "SIP Media Parameters — fields description" (page 93) for a description of the parameters.

Table 8 H.323 Media Parameters — fields description (Sheet 1 of 2)

Field	Value	Description
Preferred Codecs	G.711 -uLaw G.711 -aLaw G.729 G.723	Add codecs to the Selected list and order them in the order in which you want the system to attempt to use them. The system attempts to use the codecs in top-to-bottom sequence. **Performance note:** Codecs on all networked BCMs must be consistent to ensure the proper functionality of interacting features such as Transfer and Conference. Systems running BCM Release 3.5 or later allow codec negotiation and renegotiation to accommodate inconsistencies in codec settings over VoIP trunks.

Table 8 H.323 Media Parameters — fields description (Sheet 2 of 2)

Field	Value	Description
Enable Voice Activity Detection	<check box>	Voice Activity Detection (VAD), also known as silence suppression, identifies periods of silence in a conversation and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. If VAD is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support VAD. G.711 does not support VAD. **Performance note:** VAD on all networked BCMs and IPT systems must be consistent to ensure functionality of features such as Transfer and Conference. The Payload size on the IPT must be set to 30ms.
Jitter Buffer	Auto None Small Medium Large	Select the size of jitter buffer for your system.
G.729 payload size (ms)	10,20,30,40,50,60	Set the maximum required payload size, per codec, for the VoIP calls sent over H.323 trunks. **Note:** Payload size can also be set for Nortel IP telephones. See *BCM 4.0 Telephony Device Installation Guide* (N0060609).
G.723 payload size (ms)	30	
G.711 payload size (ms)	10,20,30,40,50,60	
Incremental payload size	<check box>	When enabled, the system advertises a variable payload size (40, 30, 20, 10 ms).
Enable T.38 fax	<check box>	When enabled, the system supports T.38 fax over IP. **Caution:** Fax tones broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. To minimize the possibility of your VoIP calls being dropped due to fax tone interference: • place the fax machine away from other telephones • turn the fax machine's speaker volume to the lowest level, or off, if available
Force G.711 for 3.1k Audio	<check box>	When enabled, the system forces the VoIP trunk to use the G.711 codec for 3.1k audio signals, such as modem or TTY machines. **Note**: You also can use this setting for fax machines if T.38 fax is not enabled on the trunk.

Table 9 SIP Media Parameters — fields description (Sheet 1 of 2)

Field	Value	Description
Preferred Codecs	G.711 -uLaw G.711 -aLaw G.729 G.723	Add codecs to the Selected list and order them in the order in which you want the system to attempt to use them. The system attempts to use the codecs in a top-to-bottom sequence. **Performance note:** Codecs on all networked BCMs must be consistent to ensure the proper functionality of interacting features such as Transfer and Conference. Systems running BCM Release 3.5 or later allow codec negotiation and renegotiation to accommodate inconsistencies in codec settings over VoIP trunks.
Enable Voice Activity Detection	<Check Box>	Voice Activity Detection (VAD), also known as silence suppression, identifies periods of silence in a conversation and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. If VAD is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support VAD. G.711 does not support VAD. **Performance note:** VAD on all networked BCMs and IPT systems must be consistent to ensure functionality of features such as Transfer and Conference. The Payload size on the IPT must be set to 30ms.
Jitter Buffer	Auto None Small Medium Large	Select the size of the jitter buffer for your system.
G.729 payload size (ms)	10,20,30,40,50,60	Set the maximum required payload size, per codec, for the VoIP calls sent over H.323 trunks. **Note:** Payload size can also be set for Nortel IP telephones. See *BCM 4.0 Telephony Device Installation Guide* (N0060609).
G.723 payload size (ms)	30	
G.711 payload size (ms)	10,20,30,40,50,60	

Table 9 SIP Media Parameters — fields description (Sheet 2 of 2)

Field	Value	Description
Enable T.38 fax	<check box>	When enabled, the system supports T.38 fax over IP. **Caution:** Fax tones broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. To minimize the possibility of your VoIP calls being dropped due to fax tone interference: • place the fax machine away from other telephones • turn the speaker volume of the fax machine to the lowest level, or off, if available

End

Configuring local Gateway parameters

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **Resources > Telephony Resources**.
4	In the **Module Panel**, select the line in which the **Actual Type** column is set to **IP Trunks**. See Figure 54 "Telephony Resources" (page 91).
5	Select the **IP Trunk Settings** tab and enter the information that supports your system. See Figure 55 "IP Trunk Settings" (page 95). Refer to Table 10 "IP Trunk Settings — fields description" (page 95) for information about the IP Trunk Settings fields.

Figure 55 IP Trunk Settings

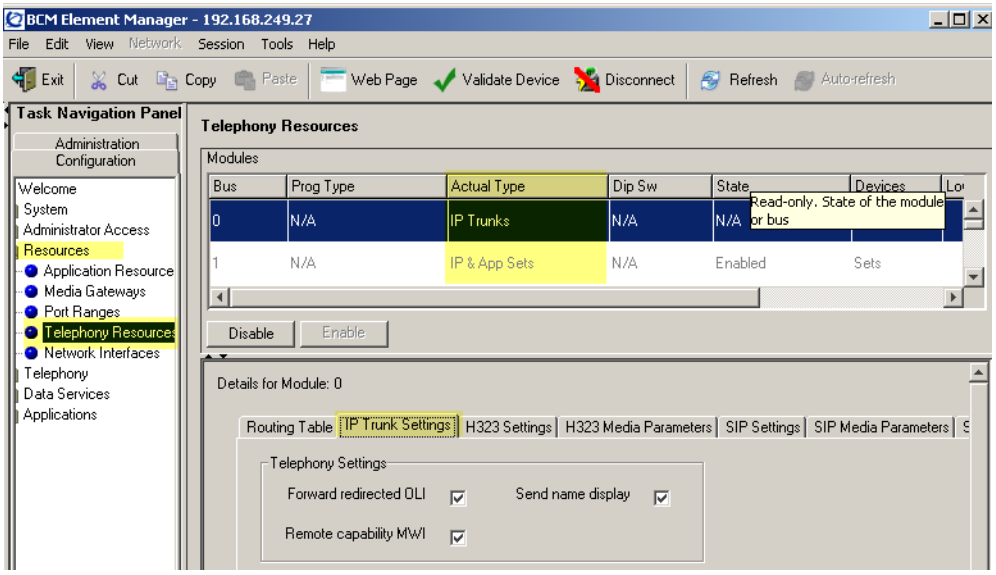


Table 10 IP Trunk Settings — fields description

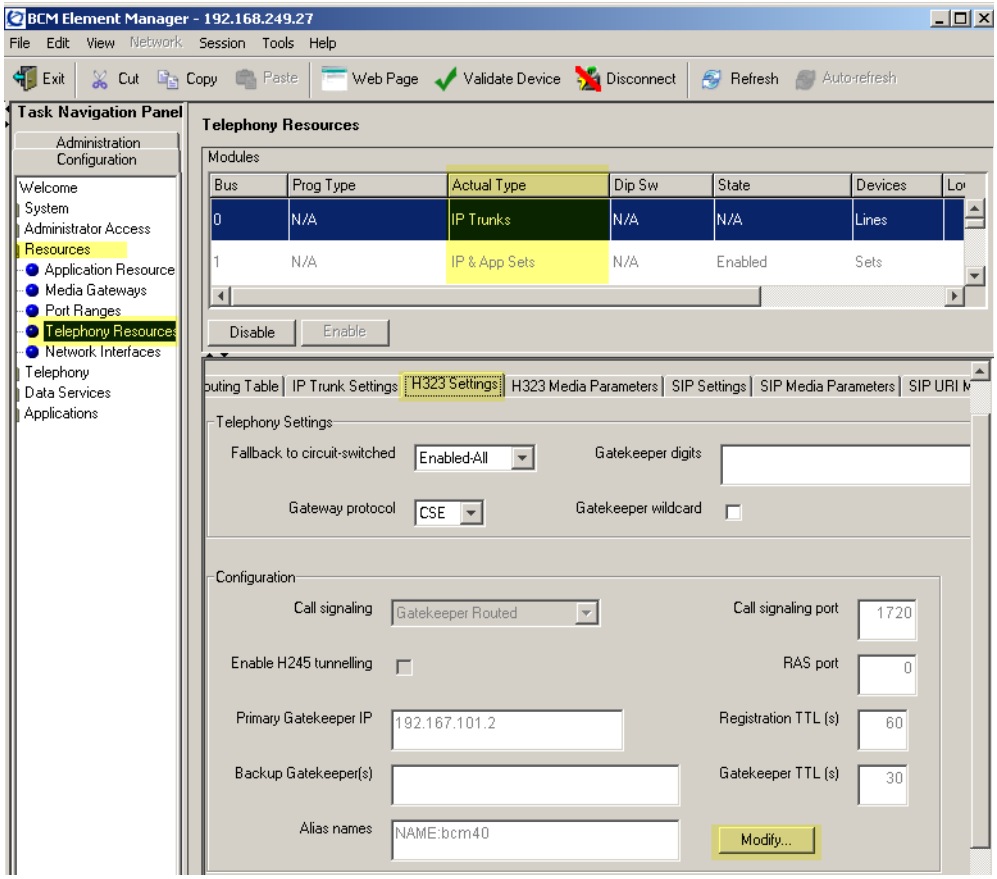
Field	Value	Description
Forward redirected OLI	<check box>	If enabled, the OLI of an internal telephone is forwarded over the VoIP trunk when a call is transferred to an external number over the private VoIP network. If disabled, only the CLID of the transferred call is forwarded.
Send name display	<check box>	If enabled, the telephone name is sent with outgoing calls to the network.
Remote capability MWI	<check box>	This setting must coordinate with the functionality of the remote system hosting remote voice mail.

6 For H.323 VoIP trunks, select the **H.323 Settings** tab.

See Figure 56 "H.323 Settings" (page 96).

Note: When implementing your dialing plan, in the H.323 Settings tab, select a value for Fall back to circuit-switched. This determines how the system handles calls if the IP network cannot be used.

Figure 56 H.323 Settings



7 For **Gateway protocol**, select **CSE**.

8 Scroll down to **Alias Name** and click **Modify**.

The Modify Call Signaling Settings page appears.

9 Enter the information that supports your system.

Refer to Table 11 "H.323 Call Signaling Settings — fields description" (page 97) for more information.

Note: Applying the changes made to the Call Signaling Settings causes all H.323 calls to be dropped. It is recommended that you make changes to the Call Signaling Settings during off-peak hours or a scheduled maintenance window.

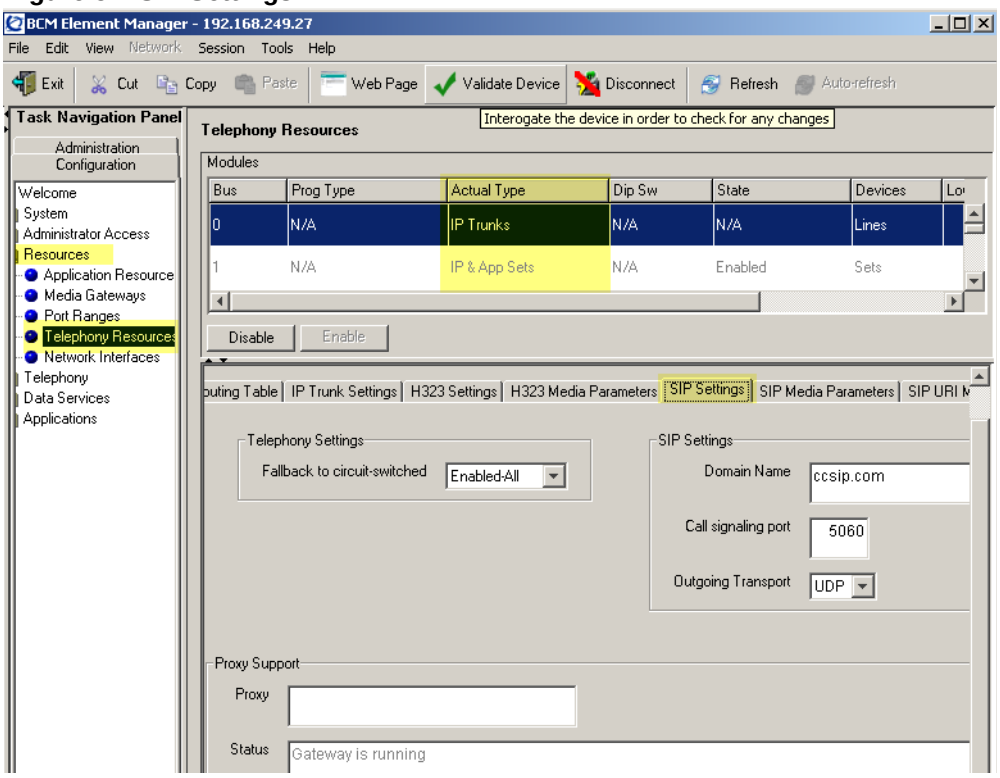
Table 11 H.323 Call Signaling Settings — fields description

Field	Value	Description
Call Signaling	Direct	Call signaling information is passed directly between H.323 endpoints. You must set up remote Gateways.
	Gatekeeper Resolved	All call signaling occurs directly between H.323 endpoints. This means that the Gatekeeper resolves the phone numbers into IP addresses, but the Gatekeeper is not involved in call signaling.
	Gatekeeper Routed	Gatekeeper Routed uses a Gatekeeper for call setup and control. In this method, call signaling is directed through the Gatekeeper.
	Gatekeeper Routed no RAS	Use this setting for a NetCentrex Gatekeeper. With this setting, the system routes all calls through the Gatekeeper but does not use any of the Gatekeeper Registration and Admission Services (RAS). Choose this option if RAS is not enabled on the NRS.
Call Signaling Port	<port value>	If VoIP applications are installed that require nonstandard call signaling ports, enter the port number here. Port number 0 means that the system uses the first available port. The default port for call signaling is 1720.
RAS Port	<port value>	If the VoIP application requires a nonstandard RAS port, enter the port number here. Port number 0 means that the system uses the first available port.
Enable H245 tunneling	<check box>	Select this field to allow H.245 messages within H.225. Restart the VoIP service for this feature to take effect.
Primary Gatekeeper IP	<IP address>	Fill in this field only if the network is controlled by a Gatekeeper. This is the IP address of the primary Gatekeeper (TLAN IP address).
Backup Gatekeeper(s)	<IP address>	NetCentrex Gatekeeper does not support RAS. Any backup Gatekeepers must be entered in this field. Gatekeepers that use RAS can provide a list of backup Gatekeepers for the endpoint to use in the event of a primary Gatekeeper failure.
Alias names	NAME:<alias name>	Enter the alias names of the BCM required to direct call signals to your system. **Note:** The Alias name is case sensitive. It must match the name configured in NRS.
Registration TTL(s)	<numeric value>	Specifies the keep-alive interval.

10 For SIP trunks, select the **SIP Settings** tab.

See Figure 57 "SIP Settings" (page 98).

Figure 57 SIP Settings



11 Enter the information that supports your system.

Refer to Table 12 "SIP Settings — fields description" for more information.

Table 12 SIP Settings — fields description

Field	Value	Description
Fallback to Circuit-Switched	Disabled	Defines how you want the system to handle calls that the system fails to send over the VoIP trunk. Enabled-TDM enables fallback for calls originating on digital telephones. This is useful if your IP telephones are connected remotely, on the public side of the BCM network, because PSTN fallback is unlikely to result in better quality of service.
	Enabled-TDM	
	Enabled-All	
Domain Name		Type the domain name of the SIP network.
Call Signaling Port	<port value>	If VoIP applications are installed that require nonstandard call signaling ports, enter the port number here. Port number 0 means that the system uses the first available port.
Outgoing Transport	UDP	
	TCP	
Proxy		If entered, all SIP calls originate to this address.
Status	Read Only	This field displays the current status of the Gatekeeper.

End

Configuring VoIP lines

Voice over IP (VoIP) lines simulate traditional Central Office (CO) lines. VoIP lines transmit data over an IP network rather than over physical lines.

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **Telephony > Lines > All Lines**.
4	Highlight the individual line you wish to configure.
5	Select the **Parameters** tab. See Figure 58 "VoIP lines".
6	Configure the **Parameters** tab appropriately for your network. Refer to Table 13 "VoIP line descriptions" for configuration information.

Figure 58 VoIP lines

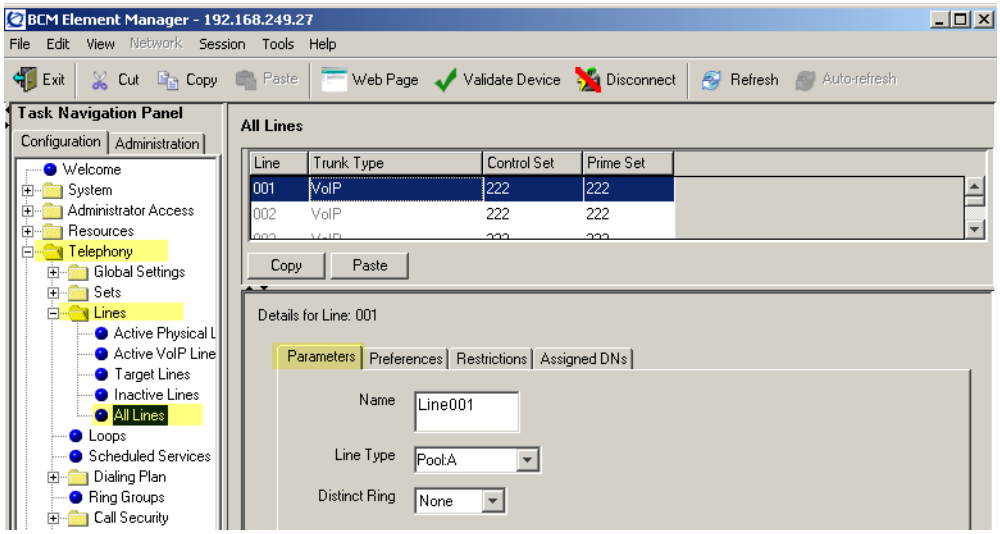


Table 13 VoIP line descriptions (Sheet 1 of 2)

Field	Value	Description
Line	001-060	Unique line number.
Trunk Type	VoIP	Ensure that the trunk type is set to VoIP when configuring VoIP lines.
Control Set		Identify a DN if you are using this line with scheduling. To change the DN, double-click the Control Set DN. For VoIP trunks, it is recommended that the Control Set be set to None because these are virtual trunks. Ensure that the VoIP trunk is assigned to a line pool.

Table 13 VoIP line descriptions (Sheet 2 of 2)

Field	Value	Description
Prime Set		Use the Prime Set if you want the line to be answered at another telephone when the line is not answered at the target telephone. To change the Prime set, double-click the Prime set DN. For VoIP trunks, it is recommended that the Prime Set be set to None because these are virtual trunks. Ensure that the VoIP trunk is assigned to a line pool.
Name		Identify the line in a meaningful way.
Line Type	Public DN:* Pool [A to O]	Defines how the line is used in relation to other lines in the system. If the line is to be shared among telephones, set to Public. If the line is assigned to only one telephone, set to DN:*. If you are using routing, put the line into line pool (A to F). If you are using line pools, configure the target lines. If your system uses both H.323 and SIP trunks, assign H.323 trunks to one pool and SIP trunks to another.
Distinct Ring	2, 3, 4, or None	For trunks assigned to line pools, set the Distinct Ring pattern to None.

7 Select the **Preferences** tab.

See Figure 59 "Preferences".

8 Configure the **Preferences** tab appropriately for your network.

Refer to Table 14 "Preferences — fields description" for configuration information.

Figure 59 Preferences

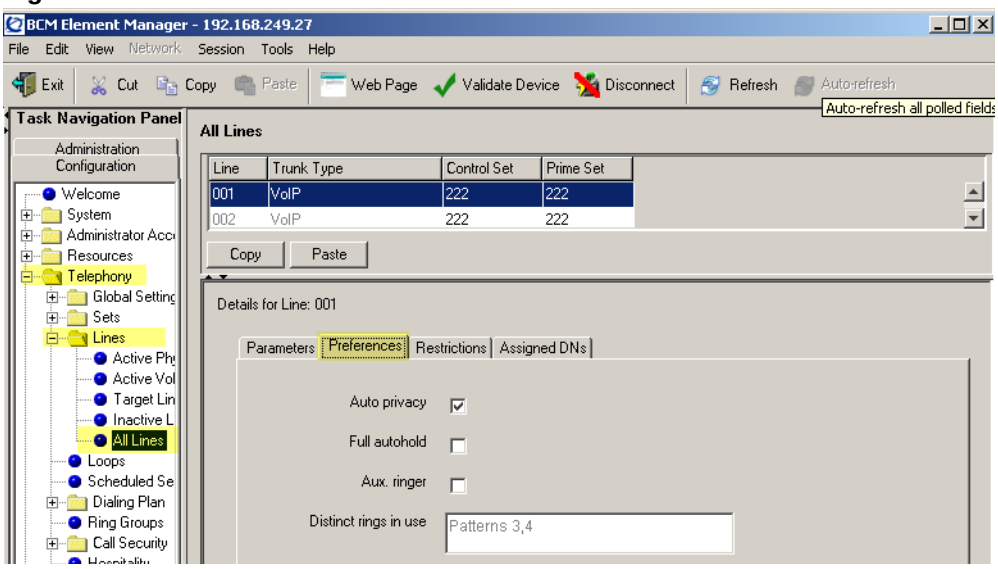


Table 14 Preferences — fields description

Field	Value	Description
Auto Privacy	<check box>	Defines whether one BCM user can select a line in use at another telephone to join an existing call. For more information, see *BCM 4.0 Device Configuration Guide* (N0060600).
Full autohold	<check box>	Enables or disables Full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if the caller selects another line. Change the default setting only if Full autohold is required for a specific application.
Aux. ringer	<check box>	If your system is equipped with an external ringer, you can enable this setting so that this line rings at the external ringer.
Distinct rings in use	Read only	Indicates whether a special ring is assigned.

9 Select the **Restrictions** tab.

See Figure 60 "Restrictions".

10 Configure the **Restrictions** tab appropriately for your network.

Refer to Table 15 "Restrictions — fields description" for configuration information.

Figure 60 Restrictions

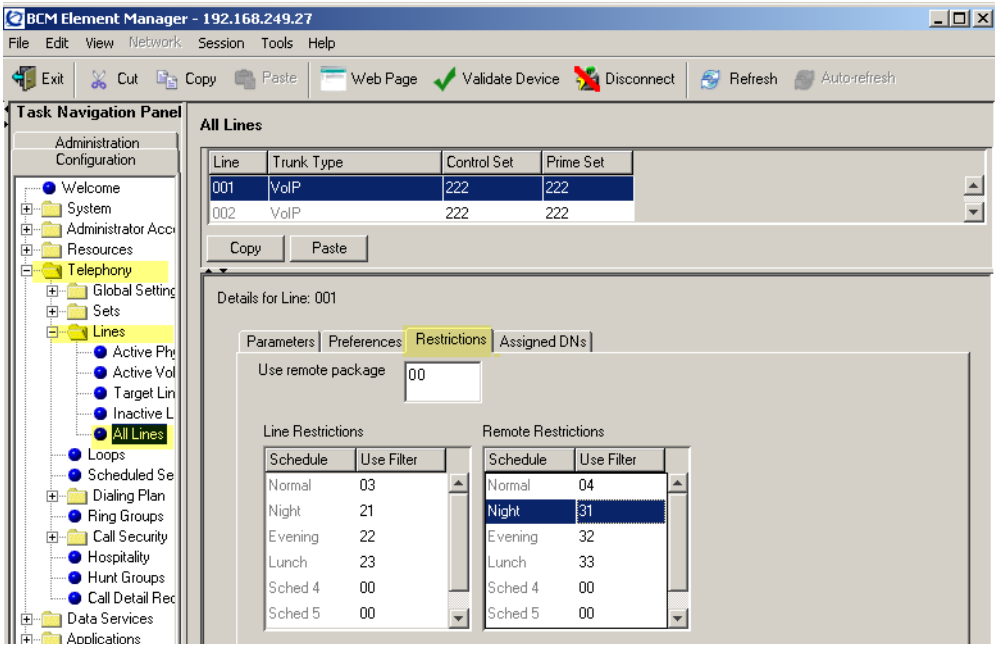


Table 15 Restrictions — fields description

Field	Value	Description
Use remote package	<remote package #>	If the line is used to receive external calls or calls from other nodes on the private network, ensure that you indicate a remote package that provides only the availability that you want for external callers. This attribute is typically used for tandeming calls.
Schedule	Default: Normal, Night, Evening, Lunch, Sched 4, Sched 5, Sched 6	
Line Restrictions - Use Filter	<00-99>	Enter the restriction filter number that applies to each schedule. These settings control outgoing calls.
Remote Restrictions - Use Filter	<00-99>	Enter the restriction filter that applies to each schedule. These settings provide call controls for incoming calls over a private network or from a remote user dialing in over PSTN.

11 Select the **Assigned DNs** tab.

See Figure 61 "Assigned DNs".

12 Edit the listed DNs or click **Add** to add a DN as required.

13 Enter the appropriate information for your network.

Refer to Table 16 "Assigned DNs" for configuration information.

Figure 61 Assigned DNs

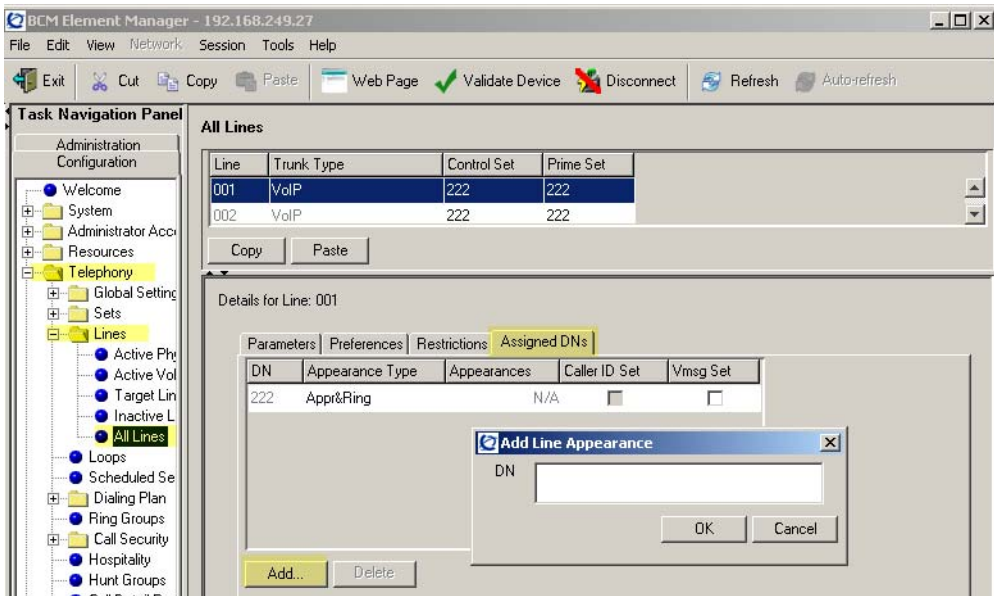


Table 16 Assigned DNs

Field	Value	Description
DN		Unique number
Appearance Type	Ring Only	Select Appr Only or Appr&Ring if the telephone has an available button. Otherwise select Ring Only.
	Appr&Ring	
	Appr Only	
Appearances		Target lines can have more than one appearance to accommodate multiple calls. For telephones that have these lines set to Ring Only, set to None.
Caller ID Set	<Check Box>	When enabled, displays caller ID for calls coming in over the target line.
Vmsg Set	<Check Box>	When enabled, an indicator appears on the telephone when a message is waiting from a remote voice mail system. Check with your system administrator for the system voice mail setup before changing this parameter.

End

Configuring target lines

Target lines are virtual communication paths between trunks and telephones on the BCM system. They are incoming lines only and cannot be selected for outgoing calls or networking applications.

Step	Action
1	Log on to Element Manager.

2 In the **Task Navigation Panel**, select the **Configuration** tab.

3 Select **Telephony > Lines** > **Target Lines**.

4 Highlight the individual line you wish to configure.

5 Select the **Parameters** tab and enter the appropriate information for your network.

See Figure 62 "Parameters" (page 104). Refer to Table 17 "Parameters — fields description" (page 104) for configuration information.

Figure 62 Parameters

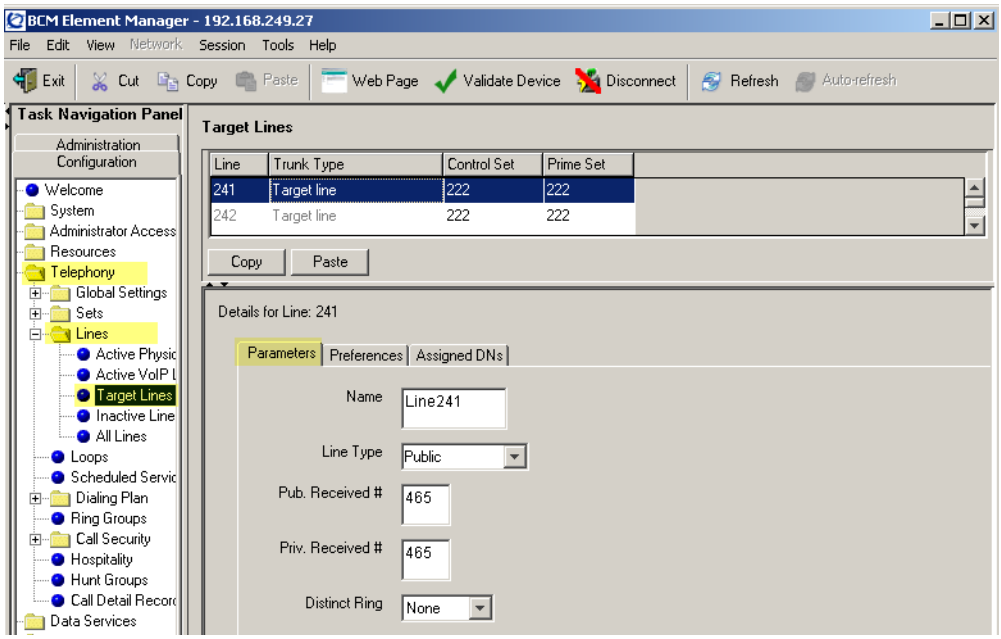


Table 17 Parameters — fields description

Field	Value	Description
Name		Type a description of the line or line function.
Line Type	Public DN:*:	If the line is to be shared among telephones, select Public. If the line is only assigned to one telephone, select DN:*:.
Pub. Received #		Confirm the existing number or enter a public received number (PSTN DID or PRI trunks) that the system uses to identify calls from the public network to the target line. The public received number cannot be the same as the beginning digits of a line pool access code or destination code.
Priv. Received #		If private network trunks (PRI or VoIP trunks) are configured, enter a private received number. The private received number specifies the digits the system uses to identify calls from the private network to a target line. This number is usually the same as the DN.
Distinct Ring	2, 3, 4, or None	If you want this line to have a special ring, select a ring pattern.

6 Select the **Preferences** tab and enter the appropriate information for your network.

See Figure 63 "Preferences" (page 105). Refer to Table 18 "Preferences — fields description" (page 105) for configuration information.

Figure 63 Preferences

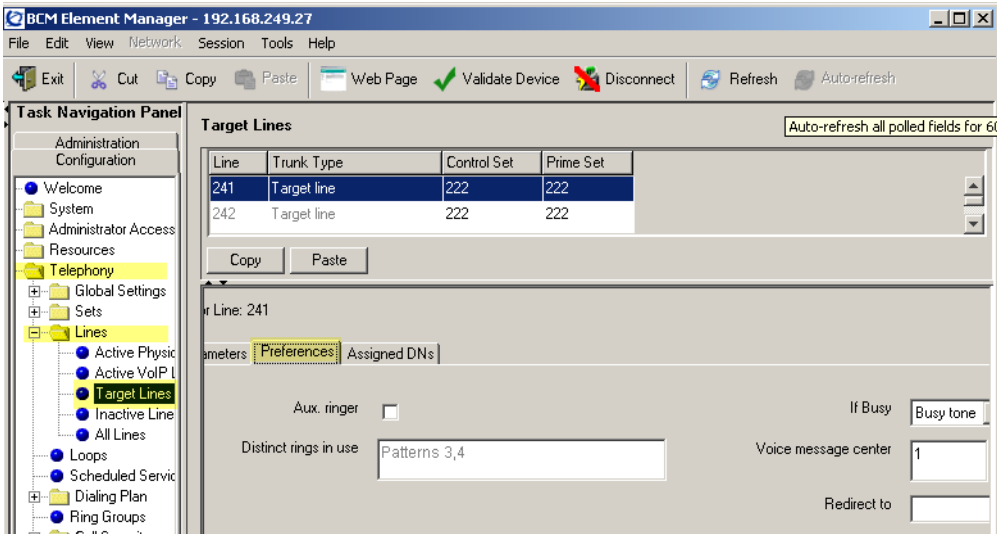


Table 18 Preferences — fields description

Field	Value	Description
Aux. Ringer	<check box>	If your system is equipped with an external ringer, you can enable this setting so that this line rings at the external ringer.
If Busy	Busy tone	To automatically direct calls to the prime telephone, select To prime. Otherwise, select Busy tone.
	To Prime	
Distinct rings in use	Read only	
Voice message center		If the system is using a remote voice mail, select the center configured with the contact number.
Redirect to		To automatically direct calls out of the system to a specific telephone, such as a head office answer attendant, enter that remote number here. Ensure that you include the proper routing information.

7 Select the **Assigned DNs** tab.

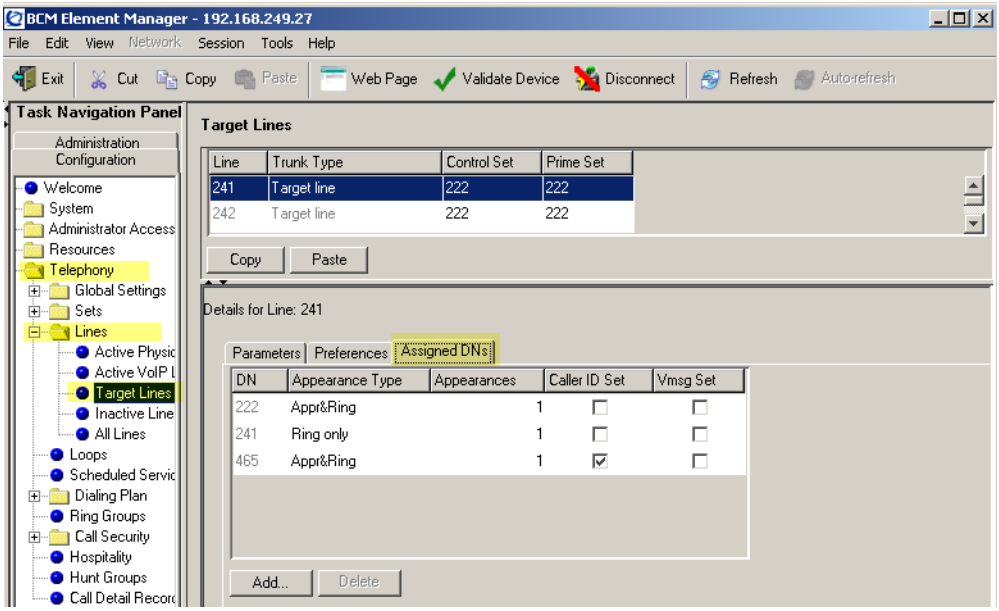
See Figure 64 "Assigned DNs" (page 106).

8 Edit the listed DNs, or click **Add** to add a DN as required.

9 Enter the appropriate information for your network.

Refer to Table 16 "Assigned DNs" (page 103) for configuration information.

Figure 64 Assigned DNs



End

Testing and troubleshooting

This chapter contains procedures to test and troubleshoot your Communication Server 1000/Business Communications Manager (BCM) integration.

The sections in this chapter are as follows:

- "Testing" (page 107)
  - "Testing the integration from the BCM system" (page 107)
  - "Testing the integration from the CS 1000 system" (page 108)
- "Troubleshooting" (page 108)
  - "BCM is unable to contact the gatekeeper at <IP address>" (page 108)
  - "Unable to complete any calls" (page 109)
  - "BCM fails to register to NRS" (page 109)
  - "Cannot make calls between the CS 1000 and BCM" (page 109)
  - "H.323 Gateway service is down" (page 110)

Testing

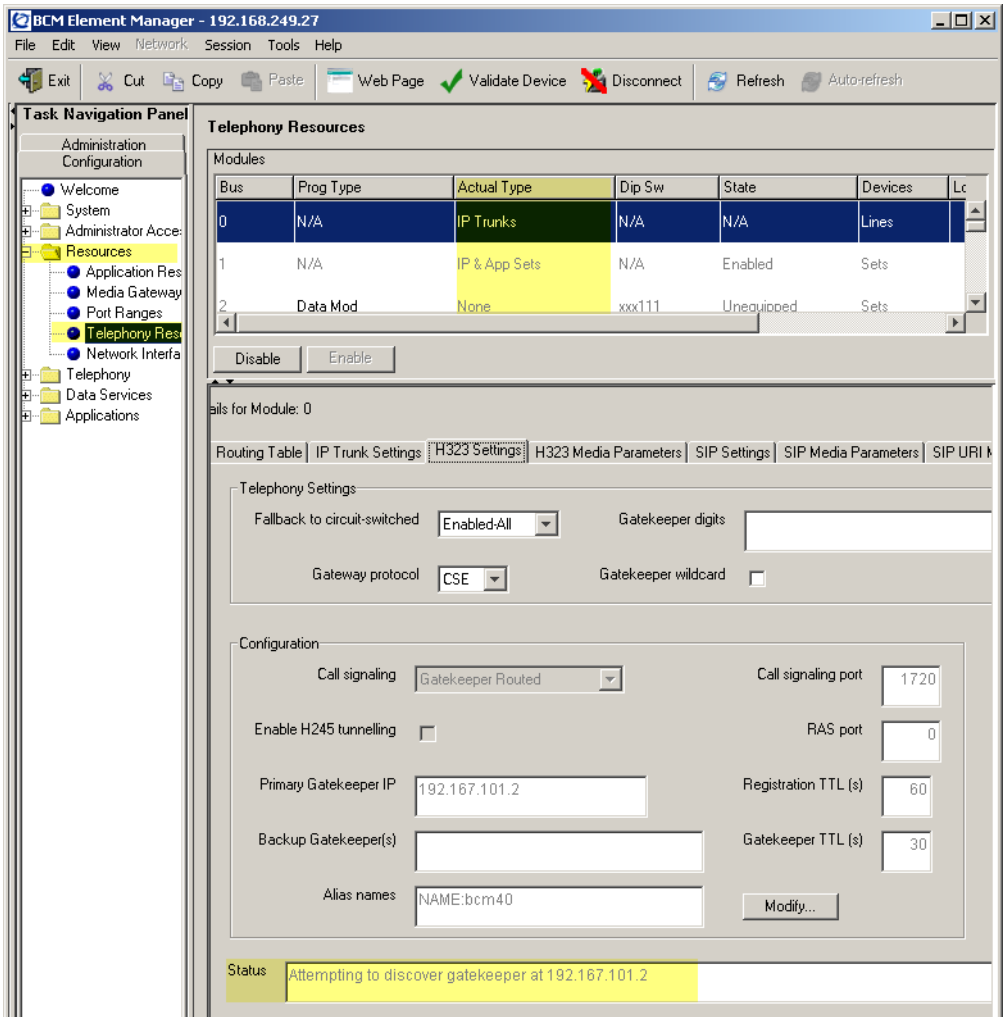
The CS 1000/BCM integration is considered successful if BCM and Network Routing Service (NRS) are able to register to each other. You can determine this from either the CS 1000 side or the BCM side.

Successful call completion is not a criterion of integration success because call completion is dependent on the dialing plan and how it is implemented. For information about dialing plans, see *Dialing Plans: Description* (553-3001-183).

Testing the integration from the BCM system

Step	Action
1	Log on to Element Manager on the BCM system.
2	Select **Resources > Telephony Resources**. See Figure 65 "Status" (page 108).
3	In the **Actual Type** column, highlight **IP Trunks**.
4	In the bottom half of the page, select the **H323 Settings** tab.
5	Scroll down to the **Status** bar to determine if the two systems are successfully registered.

Figure 65 Status



End

Testing the integration from the CS 1000 system

To determine if the two systems are registered from the CS 1000 side, check the status of the endpoints. Refer to the procedure "Checking the status of registered endpoints" (page 82).

Troubleshooting

Refer to these troubleshooting procedures to resolve common integration issues.

BCM is unable to contact the gatekeeper at <IP address>

Step	Action
1	Check whether you are able to ping the Gatekeeper across the network. If not, a routing issue can exist in your network. Contact your network administrator to resolve any routing issues.
2	Check that the correct Gateway endpoint IP address is configured in BCM. You may need to reset the feps service under the Service Manager.

3	Check that the correct Gateway endpoint IP address is configured in the CS 1000.
4	Check that the Alias name is properly configured in BCM. The alias name is case sensitive and must match exactly what is configured in the CS 1000.
5	Check that the Gateway protocol is set to **CSE**.

End

Unable to complete any calls

Step	Action
1	Check whether the BCM and Gatekeeper have established connectivity. If not, ensure that the BCM and NRS can communicate with each other.
2	Check that the line is configured for outgoing calls. DNs need to have lines configured for both incoming and outgoing calls. Check your networks dialing plan or see *Dialing Plans: Description* (553-3001-183).
3	Verify that the dialing plan has been properly implemented on both the CS 1000 and BCM. For more information about dialing plans, see *Dialing Plans: Description* (553-3001-183).

End

Cannot make calls between the CS 1000 and BCM

Symptoms:

- calls between the CS 1000 and BCM fail
- CDP calls fail
- no channel/circuit is available

Step	Action
1	Verify your dialing plan and call routing.
2	On the BCM, log on to Element Manager and select **Telephony > Dialing Plan > Private Network**.
3	Verify that **Private Network Type** is set to **CDP**.
4	Ensure that packets are not blocked by your network firewall.

End

BCM fails to register to NRS

Symptoms:

- BCM fails to register to the NRS
- calls fail between the CS 1000 and BCM in both directions

Step	Action
1	Check whether you can ping the BCM from the NRS command line. If unsuccessful, check your network settings. Note that the NRS does not respond to pings.
2	In the **H323 Settings** tab for **IP trunks** under **Resources > Telephony Resources**, verify that the BCM includes its alias name as “NAME:aliasname”.
3	Verify that the **Alias** names match on the NRS and BCM.
4	In the **H323 Settings** tab for **IP trunks** under **Resources > Telephony Resources**, make sure the Gateway protocol is set to **CSE**.
5	Verify that the NRS has the proper routing entries.
	End

H.323 Gateway service is down

Symptoms:

- VoIP H.323 Gateway service is down
- VoIP Gateway cannot be started manually
- VoIP Gateway does not start after a reboot or power cycle

Step	Action
1	On the BCM, log on to Element Manager.
2	Select **Resources > Telephony Resources**.
3	In the **Actual Type** column, highlight **VoIP Trunks**.
1	Select the **H.323 Settings** tab and verify that the **Call Signaling Port** is set to **1720**.
2	Check that the BCM and NRS can register with each other. Refer to "Testing the integration from the BCM system" (page 107).
	End

Solution Integration Guide for Communication Server 1000/Business Communications Manager

CS 1000/BCM

Document Number: **NN43001-326**
Document Status: **Standard**
Document Version: **01.02**
Release Date: **25 October 2006**

Copyright © 2006 Nortel Networks. All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, Nortel (Logo), the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

NORTEL